

Network Probe User Guide

Network Probe User Guide

Table of Contents

1. Introduction	1
2. Installation	2
Windows installation	2
Linux installation	3
Mac installation	4
Deployment	5
System requirements	6
3. Main	8
Overview	8
Windows	8
Top n windows	10
Summary window	11
My Windows	12
Alarm windows	12
Profiles	14
Profiles	14
Profile Manager	14
Switch profiles	14
4. Traffic Statistics	16
Overview	16
Applet interface overview	16
Switching network traffic view	17
Detaching a tab to a window	18
Collapsing and resizing a table column	19
Changing the data in the charts	19
Sorting a table column	21
Searching for network traffic details	21
Filtering network traffic details	22
Viewing more detail	23
Exporting network traffic data	23
Protocols	24
Hosts	26
Conversations	27
Protocols per host	29
Protocols per conversation	31
Network cards	33
Network card conversations	35
Network	37
Alarms	38
5. Traffic Log	40
Overview	40
Display logged statistics	40
Logged interval data	41
Log manager	42
6. Alarms	44
Alarms	44
Adding alarms	44
Edit alarms	47
Remove alarms	48
7. Setup	50
Overview	50
Collected statistics	50
Reset interval	51

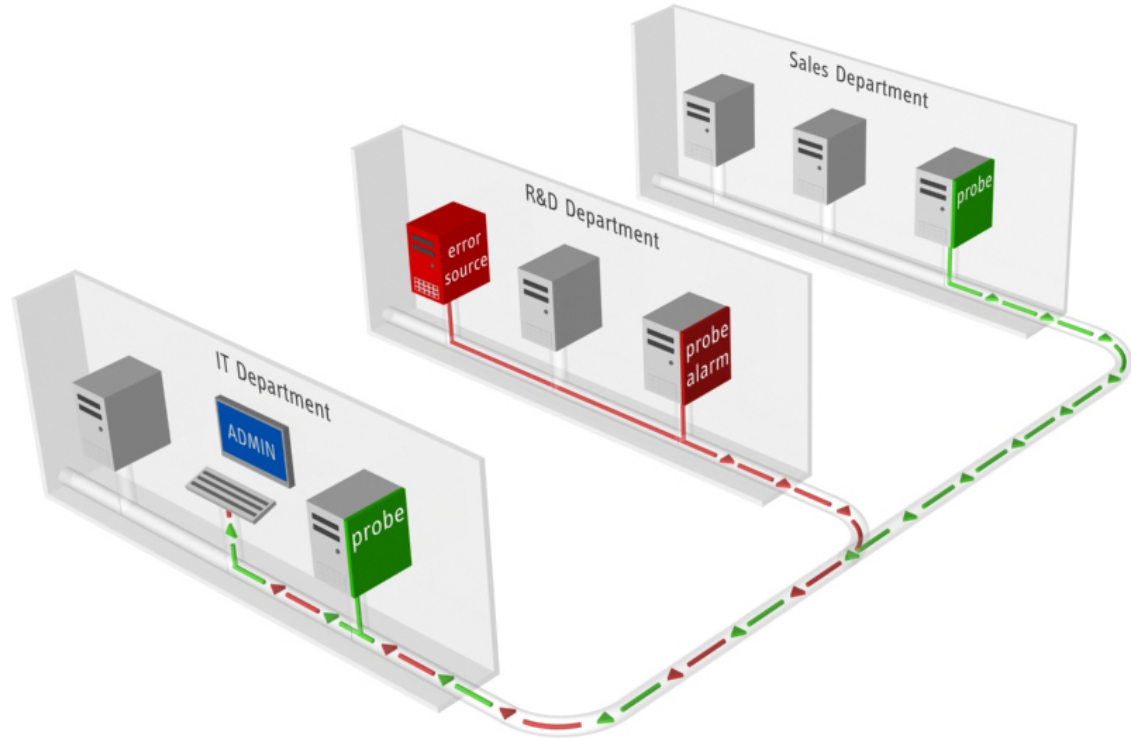
Network interface	52
Host name resolving	52
Users and passwords	52
Filters	55
Ethernet address filters	55
IP address filters	56
Protocol filters	56
8. Advanced	58
Manually starting the probe	58
Starting the stand-alone client	58
Command line options	58
Resetting the admin password	59
Dump packet content to the console	60
Running the probe as a Windows service	61
Automatically starting the probe on *NIX	61
Configure web browsers to use Java (Linux)	62
Starting the probe with no IP assigned to the interface	62
Performance tuning	63
9. Practical Use	64
Slow network	64
Monitoring	66

List of Tables

2.1. Supported browsers	6
4.1. Filter operators	22

Chapter 1. Introduction

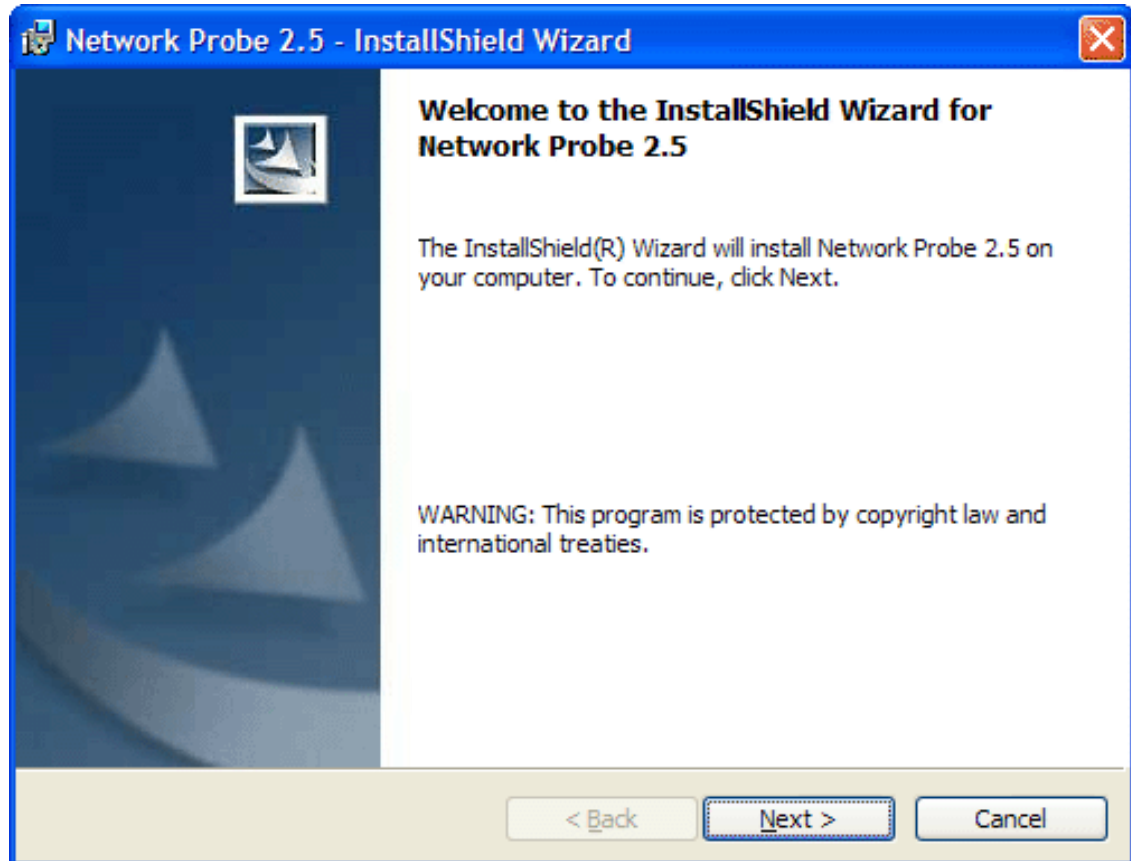
Network Probe is a network traffic monitor and protocol analyzer that gives you an instant picture of the traffic situation on your network. It displays detailed information about the type and amount of network traffic, and helps you identify potential problems and bottlenecks in your computer networks.



Chapter 2. Installation

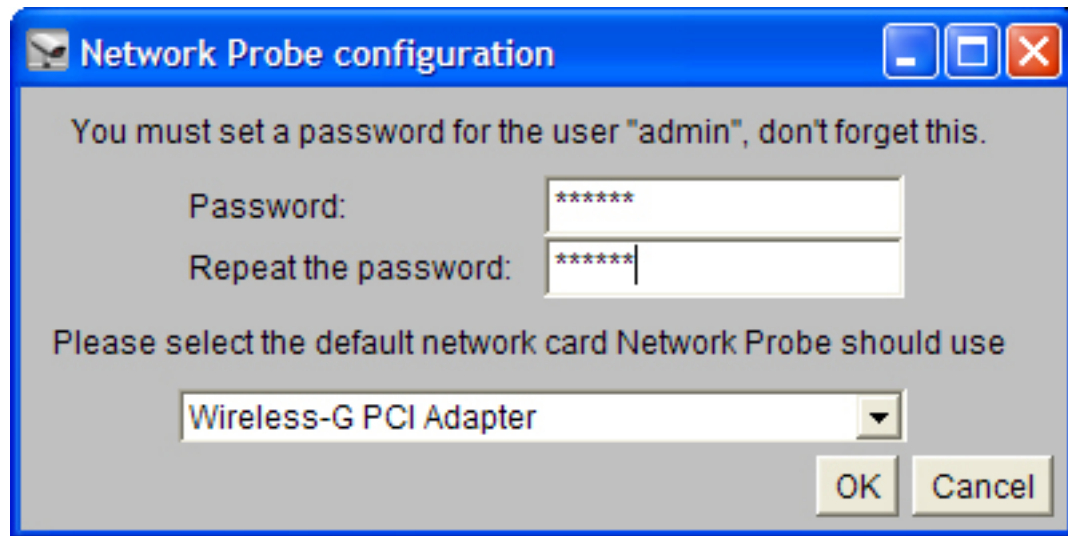
Windows installation

Double click the Network_Probe_2.x-install.exe file and follow the instructions.



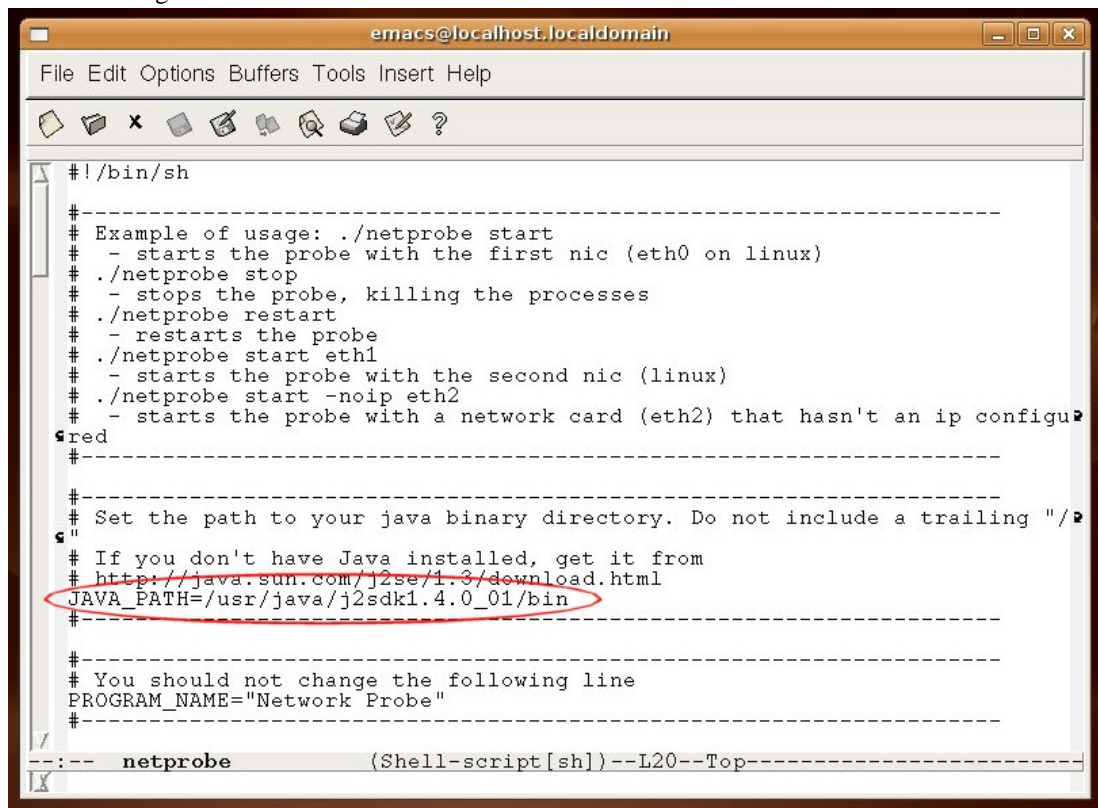
During the installation, a packet driver will be installed as well. A restart of the computer is required after installation is done, otherwise the packet driver won't start. The 2.x version will not overwrite any existing 1.x versions. If you have a 1.x version installed, you can copy the file "Program Files/Network Probe/config/config.txt" to "Program Files/Network Probe 2/config/config.txt", to keep old configurations. Any logged data from the 2.x version can also be copied from "Program Files/Network Probe/statistics" to "Program Files/Network Probe 2/statistics".

The first time Network Probe is started, you are prompted to set a password for the "admin" user.



Linux installation

1. Open a terminal window and change to the directory where you downloaded netprobe-xxx.tar.gz. Unpack the file by typing "gzip -cd netprobe-xxx.tar.gz |tar xvf -".
2. Change to the newly created netprobe directory and open the "netprobe" file in a text editor. Locate the line starting with JAVA_PATH= and insert the full path to your Java binary directory. Do not include a trailing "/".



3. To start the probe, type "./netprobe start". You need to be logged in as root to run Network Probe. The

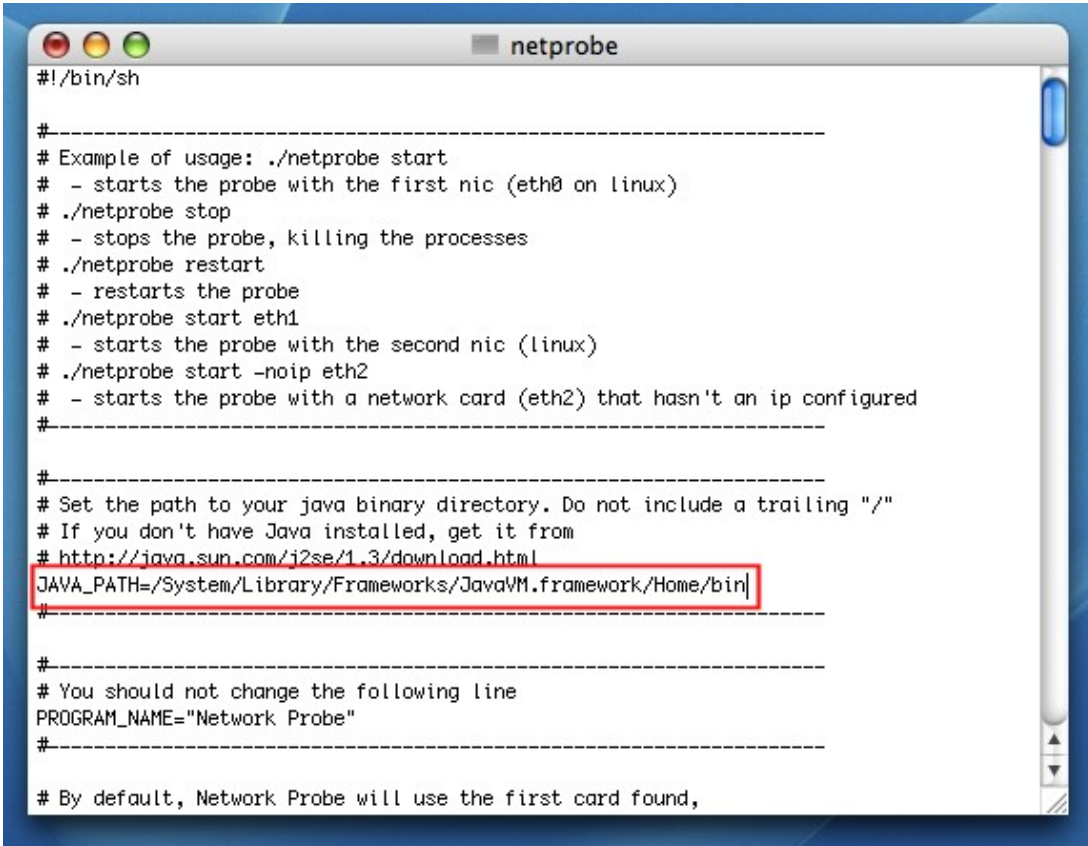
first time you start Network Probe, you will be asked to set a password for the admin user.

Startup parameters can be set in the line starting with `STARTUP_PARAMETERS=`, located in the file "netprobe".

To keep configurations from older versions of Network Probe, copy the file "config.txt" from the config folder in your old Network Probe directory to the config folder in the new Network Probe directory. Any logged data data from version 2.x can also be copied from the old statistics folder into the new statistics folder.

Mac installation

1. Unpack the downloaded netprobe-xxx.tar file by double clicking it.
2. Open the newly created netprobe directory and open the "netprobe" file in a text editor. Locate the line starting with `JAVA_PATH=` and insert the full path to your Java binary directory. Do not include a trailing `"/`.



```
#!/bin/sh

#-----
# Example of usage: ./netprobe start
# - starts the probe with the first nic (eth0 on linux)
# ./netprobe stop
# - stops the probe, killing the processes
# ./netprobe restart
# - restarts the probe
# ./netprobe start eth1
# - starts the probe with the second nic (linux)
# ./netprobe start -noip eth2
# - starts the probe with a network card (eth2) that hasn't an ip configured
#-----

#-----
# Set the path to your java binary directory. Do not include a trailing "/"
# If you don't have Java installed, get it from
# http://java.sun.com/j2se/1.3/download.html
JAVA_PATH=/System/Library/Frameworks/JavaVM.framework/Home/bin
#-----

#-----
# You should not change the following line
PROGRAM_NAME="Network Probe"
#-----

# By default, Network Probe will use the first card found,
```

3. To start the probe open a terminal and change to the newly created netprobe directory. Type `./netprobe start`. You need to be logged in as root to run Network Probe. The first time you start Network Probe, you will be asked to set a password for the admin user.

Startup parameters can be set in the line starting with `STARTUP_PARAMETERS=`, located in the file "netprobe".

To keep configurations from older versions of Network Probe, copy the file "config.txt" from the con-

fig folder in your old Network Probe directory to the config folder in the new Network Probe directory. Any logged data from version 2.x can also be copied from the old statistics folder into the new statistics folder.

Deployment

The Home Edition (free) of Network Probe supports single-computer mode only, so only traffic going from/to the computer where Network Probe is installed will be picked up. It can be connected to a normal port on the switch.

For full utilization of Network Probe, a license key is required, which will enable promiscuous mode. Promiscuous mode means that it can pick up all network packets which the network card sees. Make sure you install the probe on a computer with a network card capable of promiscuous-mode operation. If the card does not support promiscuous mode, a warning is shown on the login screen (also in Home Edition):

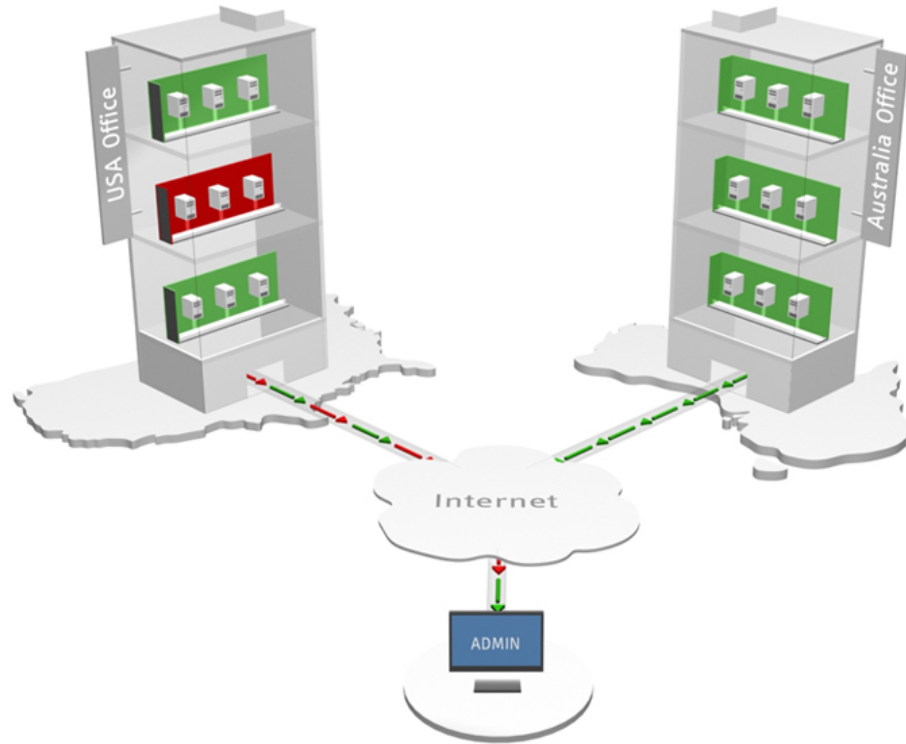


The computer should be connected to a mirrored port on your network switch, also known as a SPAN (Switched Port Analyzer) port. The normal operation of a switch is to send packets only to the computer they destinate to, but a SPAN port receives a copy of all packets going through the switch. A SPAN port is normally available on managed switches only.

It is also possible to use Network Probe on a wireless network, as long as the wireless NIC supports promiscuous mode.

After installation, you can log on to the probe using any web browser from any computer having access to port 7030 on the computer where Network Probe is installed.

Strategically install a copy of Network Probe on each subnet you want to monitor, and log in remotely from a single central location.



System requirements

- Windows XP, Windows Vista, Windows 2000, Windows 2003, Linux, FreeBSD, MacOS X, Solaris (with root access)
- Sun Java Runtime Environment 1.3 or higher. GNU Java is not fully supported yet
- A web browser with JavaScript enabled. Java plug-in required for access to "Traffic Statistics" and "Traffic Log"
- A network card supporting promiscuous mode, if connected to a SPAN port
- Recommended hardware is at least a 2GHz CPU and 1 GB of RAM

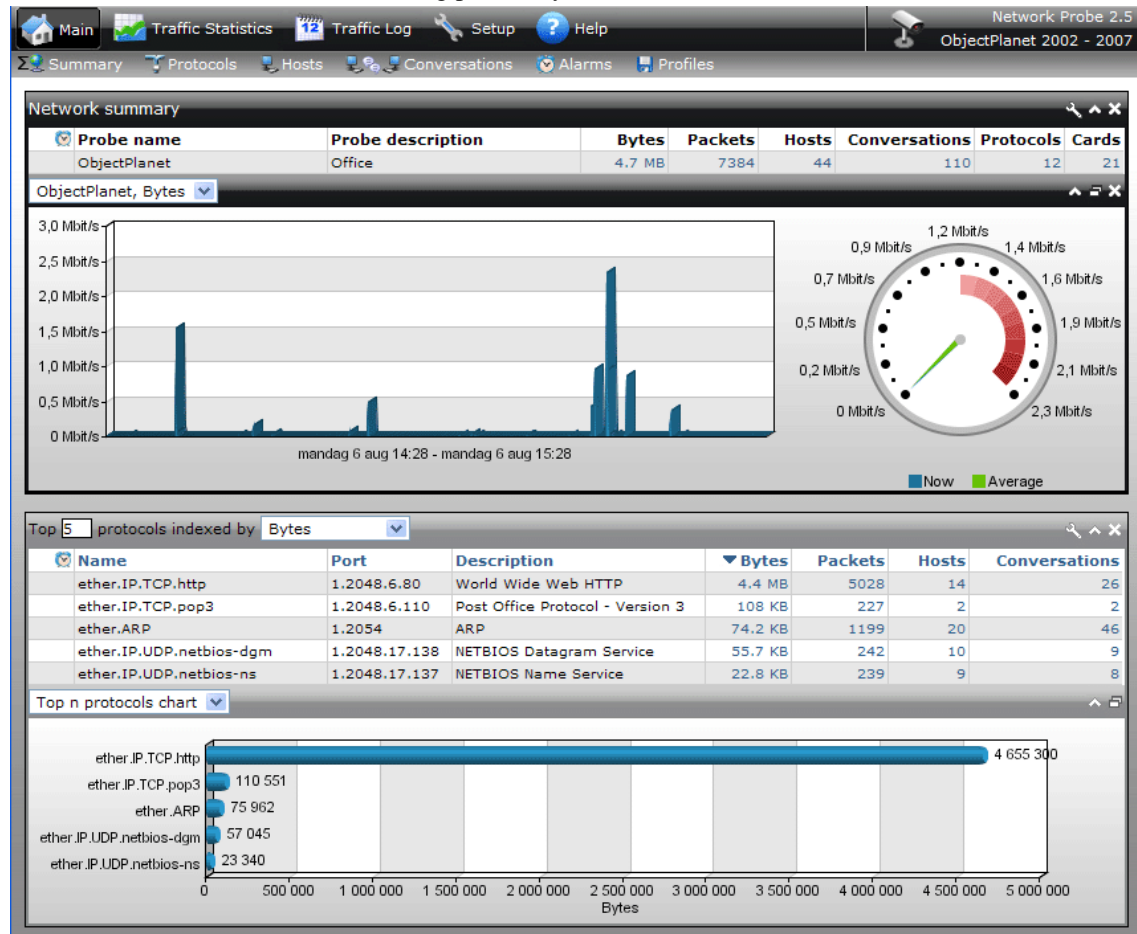
Table 2.1. Supported browsers

Platform	Browser	Version
Windows	Internet Explorer	6 and newer
Windows	Firefox	1.5 and 2.0
Windows	Opera	8.54
Linux	Firefox	1.5 and 2.0
Mac	Firefox	2.0

Platform	Browser	Version
Mac	Camino	1
Mac	Safari	2

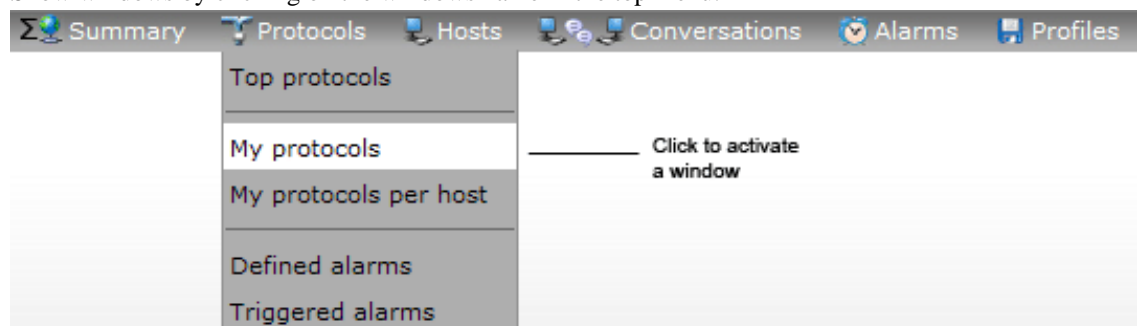
Chapter 3. Main Overview

The Main screen gives you an instant overview over the total network throughput, top protocols, hosts, talkers listeners and conversations taking place on your network.

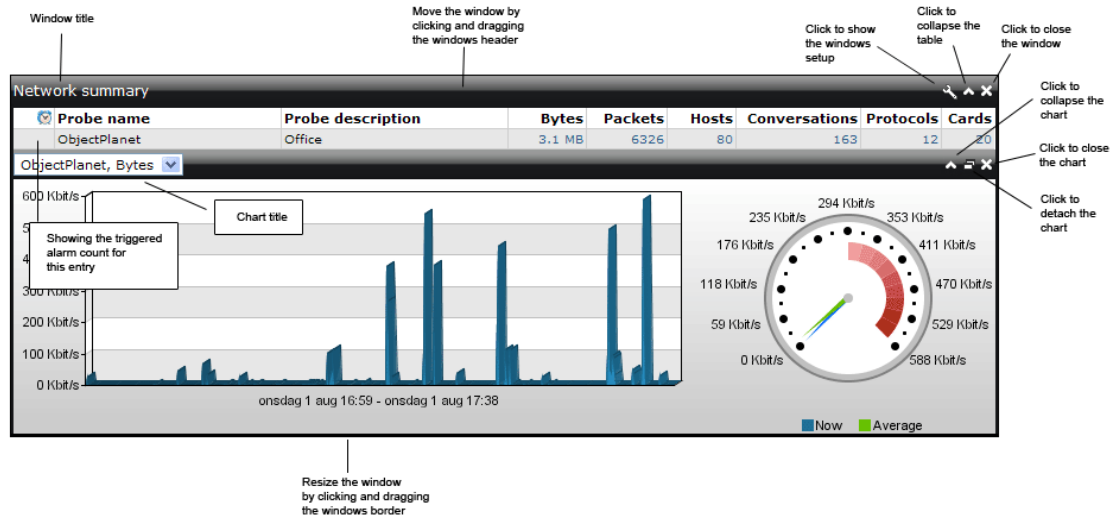


Windows

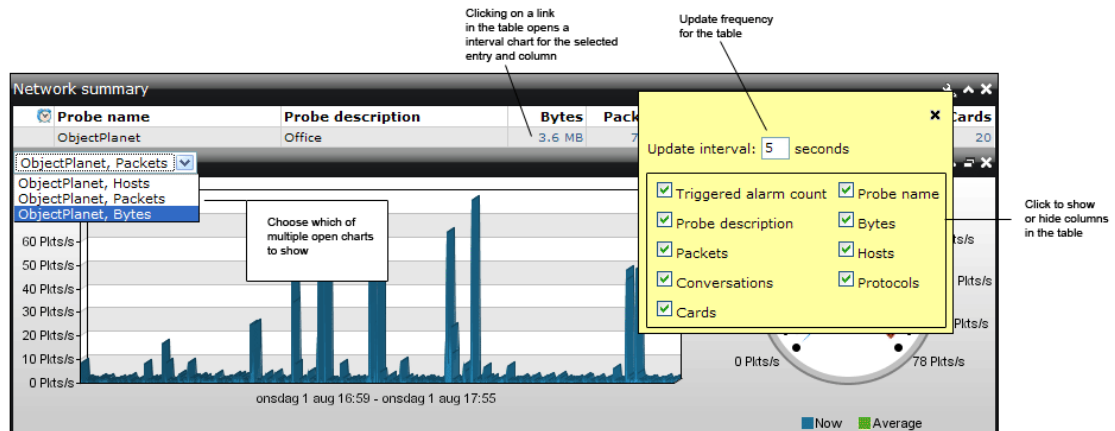
Show windows by clicking on the windows name in the top menu.



Each window contains two sections. The top section contains a table, and the bottom section a chart. Windows can be customized in a variety of ways.



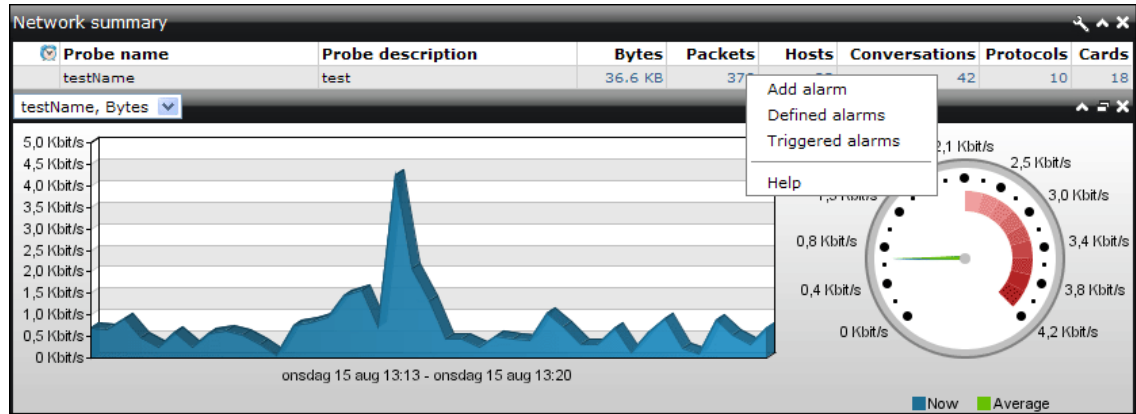
The table can be customized through the windows setup screen. Clicking links in the table opens an interval chart for the selected entry and column. Which of the multiple open charts to display can be chosen in the drop down box between the chart and the table. Interval charts are updated when there is a new interval available at the server.



Window right click menu

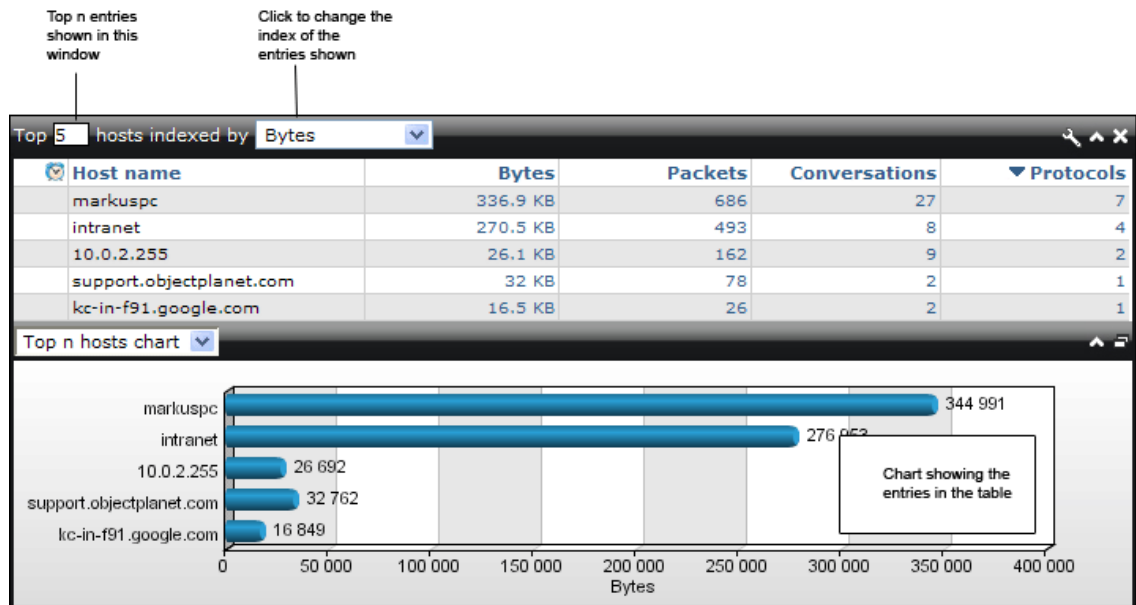
Each window has a right click menu which lets you manage alarms for the windows table.

- **Add alarms** - this will open the add alarm window, and fill in the entry clicked on.
- **Defined alarms** - this will open a window showing the defined alarms for this windows table.
- **Triggered alarms** - this will open a window showing the triggered alarms for this windows table.

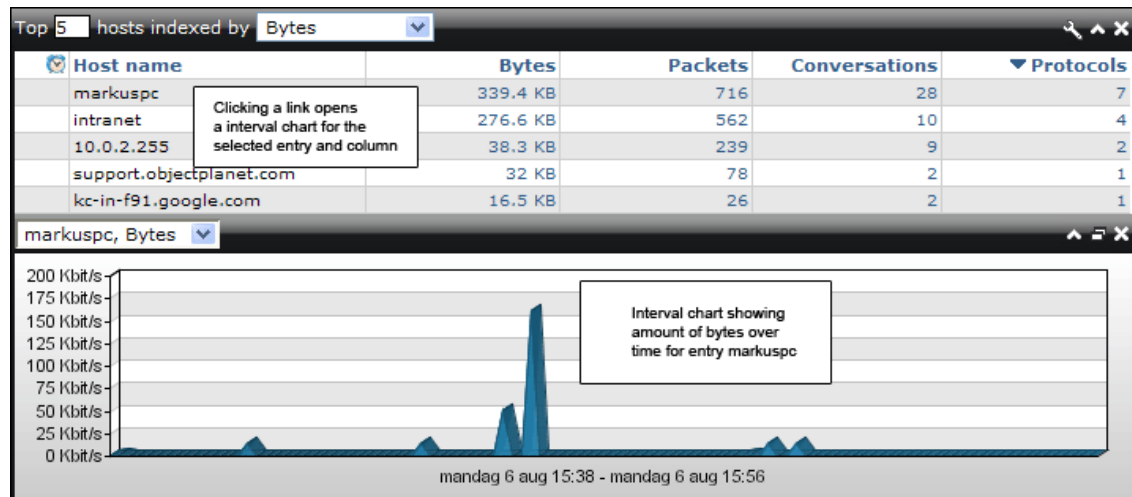


Top n windows

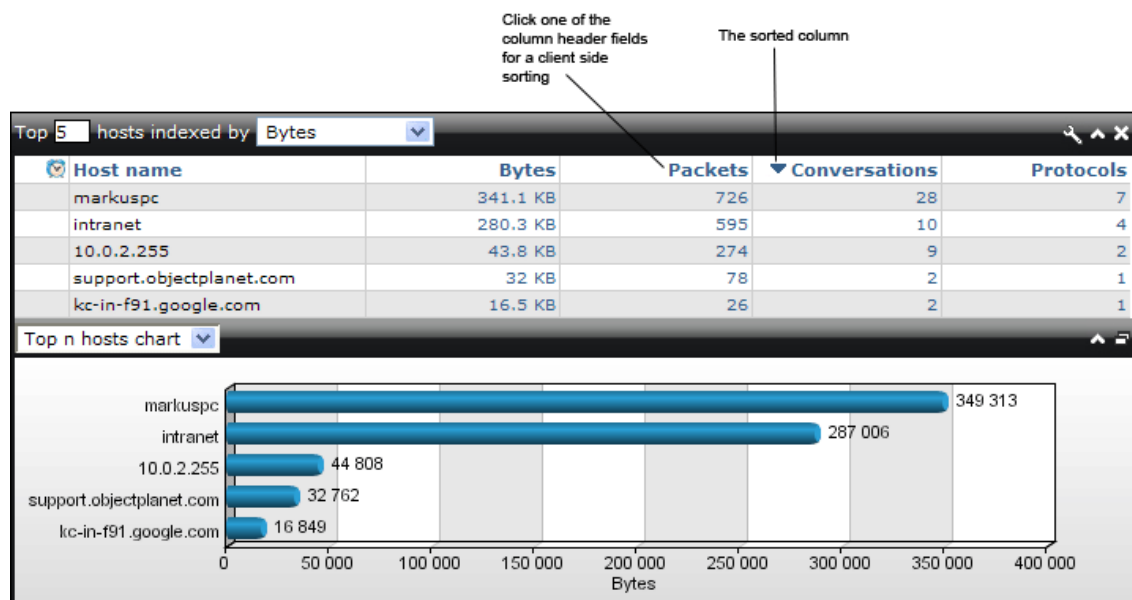
Using the top n windows you can watch the top n protocols, hosts, talkers, listeners and conversations on your network. Per default the top n data is indexed by the amount of traffic the entries have. You can change the index to the number of packets, the number of hosts, conversations or protocols. The amount of entries displayed in the table can be changed in the input field in the window header. The top n chart at the bottom of window displays the entries in the table graphically.



Clicking on a link in one of the top n tables will open an interval chart. Interval charts displays traffic over time for the selected interval.

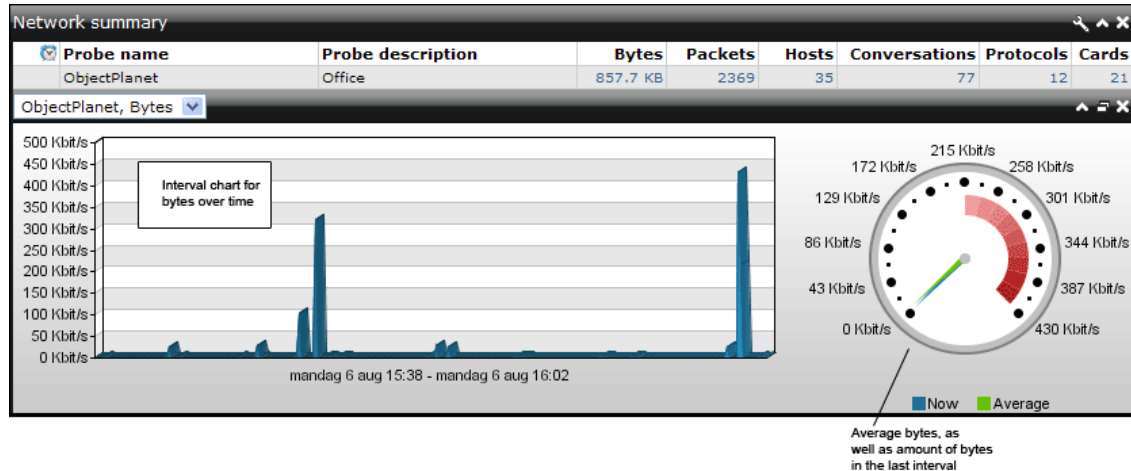


Clicking one of the column header fields in a top n table sorts the table in descending order, with the largest values at the top. Click the column header again to sort in the opposite direction. The sorting done is a client sorting as opposed to changing the tables index. Changing the tables index reloads the top n data from the server with the new index.

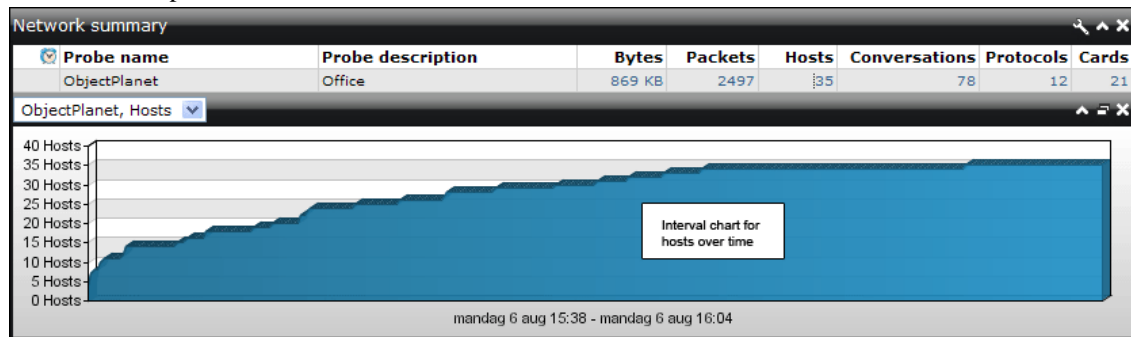


Summary window

The summary window lets you monitor the total throughput, the number of packets, hosts, conversations, protocols and network cards on the network. Charts for bytes and packets consists of two charts, one line chart and one gauge chart. The line chart displays the bytes or packets over time, while the gauge chart shows the average amount of bytes or packets as well as the field's value in the last interval.

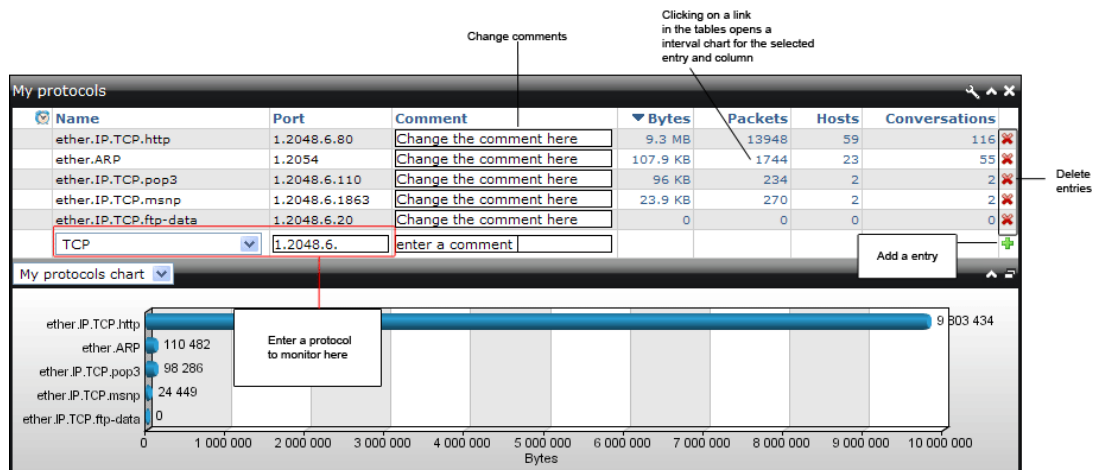


Interval charts for conversations, protocols and network cards are line charts and show the amount of conversations, protocols or network cards over time.



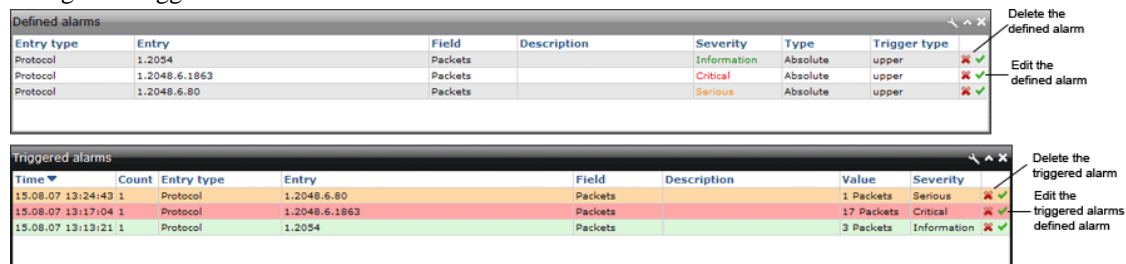
My Windows

My Windows let you easily monitor protocols, hosts and conversations of your choice. Comments can be added to each entry, and can be changed at any time later on. Add an entry by clicking the add entry button or pressing enter in one of the input fields, and delete it by clicking the delete button.

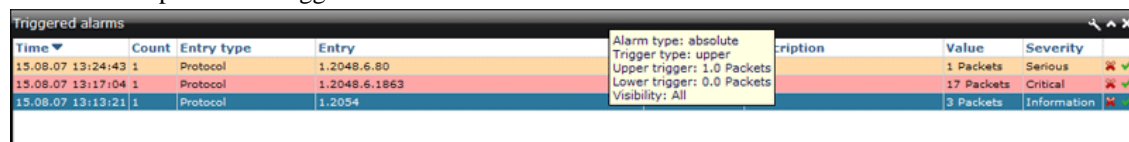


Alarm windows

In the "Main" screen both windows for defined and triggered alarms are available. Those windows can contain all triggered or defined alarms or alarms for a specific table. In the "Defined alarms" window you can view and manage the defined alarms. The "Triggered alarms" windows show the triggered alarms color coded by its severity. In the "Triggered alarms" window you can delete triggered alarms, and change the triggered alarms defined alarm.



Both the triggered and the defined alarm windows feature a tooltip if you hold the mouse over a entry. The tooltip shows detailed information about the alarm entry not shown in the table. The below image shows a tooltip for the "Triggered alarms" window.



Defined alarm windows popup menu

Right click on a alarm entry in the one of the defined alarm windows to view the popup menu.

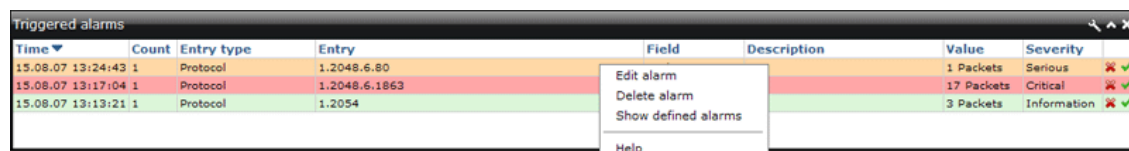
- **Edit alarm** - this will let you edit the clicked defined alarm entry.
- **Delete alarm** - this will delete the clicked defined alarm entry.
- **Show triggered alarms** - this will show the triggered alarms.



Triggered alarm windows popup menu

Right click on a alarm entry in the one of the triggered alarm windows to view the popup menu.

- **Edit alarm** - this will let you edit the clicked alarms defined alarm.
- **Delete alarm** - this will delete the clicked triggered alarm entry.
- **Show defined alarms** - this will show the defined alarms.



Profiles

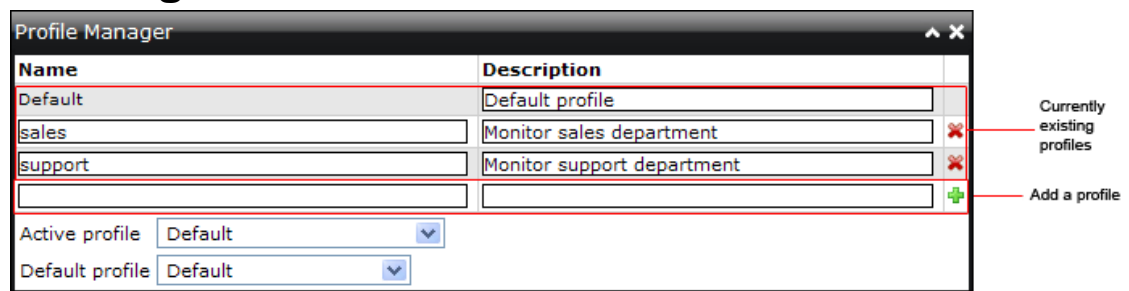
Profiles

A profile stores the Main screen layout of windows and tables. By activating a profile the Main screens windows and tables are arranged as they were the last time the profile was saved. Each user can easily create, edit and switch active profiles using the profile manager.

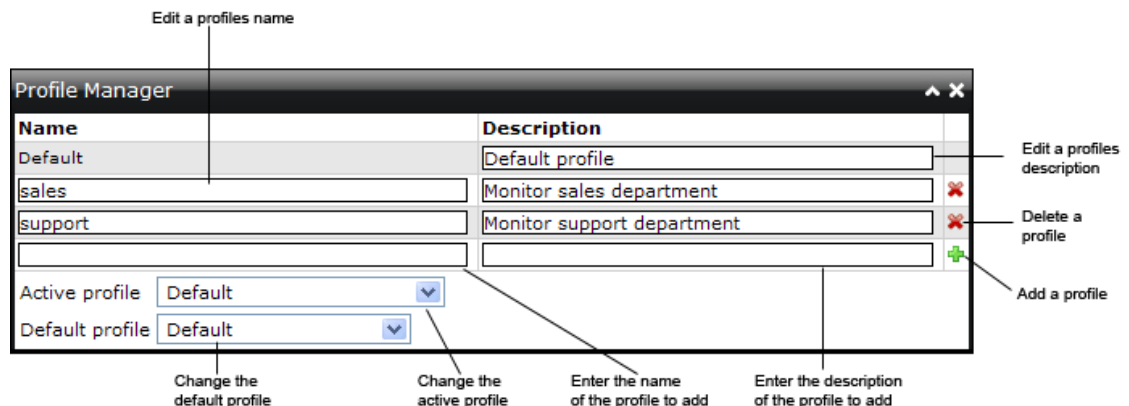
The default profile is the profile that is activated when a user logs on to the probe and can be changed in the "Profile Manager" window.

Each user can create an arbitrary number of profiles. Using multiple browser windows, users can have multiple active profiles at the same time.

Profile Manager

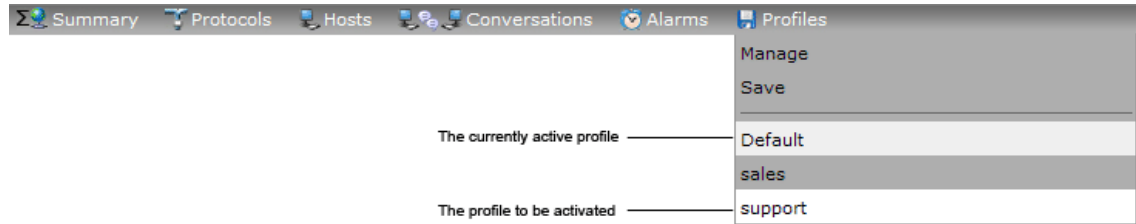


The "Profile Manager" window can be used to add, edit and delete profiles. In the "Profile Manager" window you can also change the active and the default profile. The default profile is the profile activated when you log on.

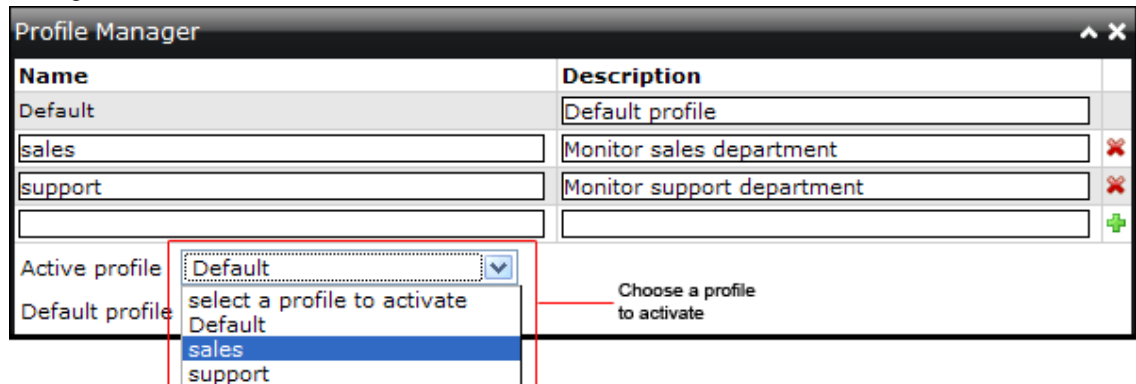


Switch profiles

Profiles can be activated either from the top menu or the "Profile Manager" window. To activate a profile from the top menu, click the profiles name. The name of the current active profile is highlighted in the menu.



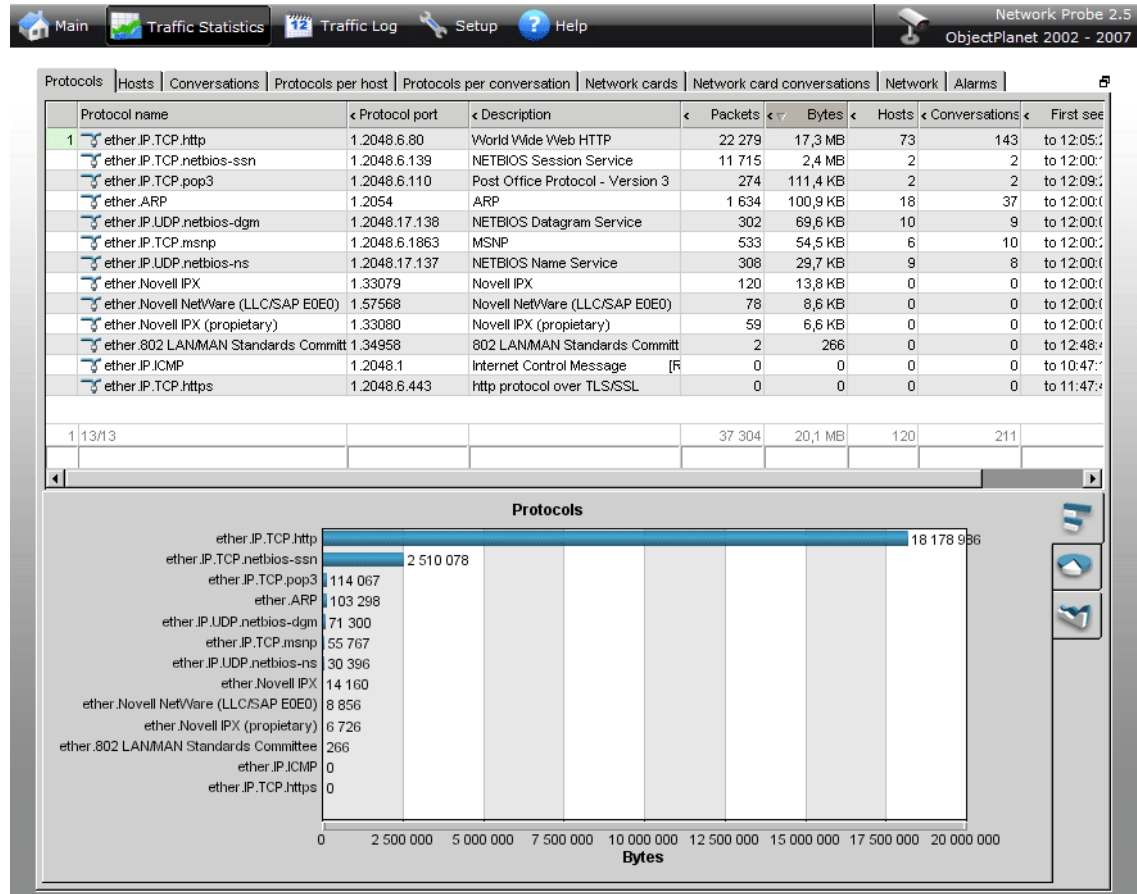
Choose one of the options in the Active profile dropdown box to activate a profile from the "Profile Manager".



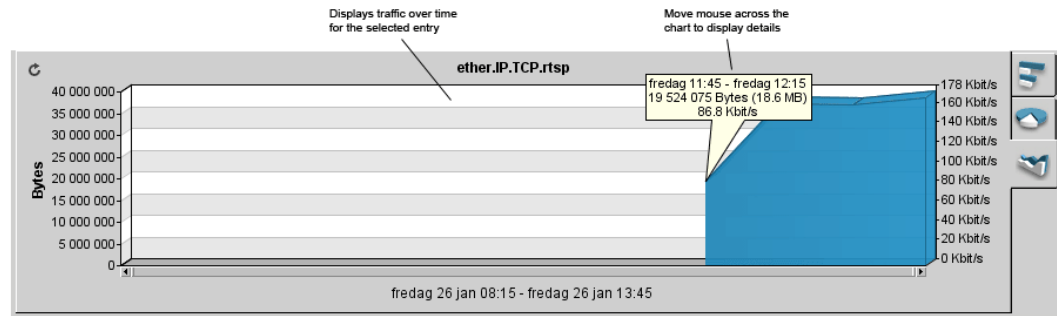
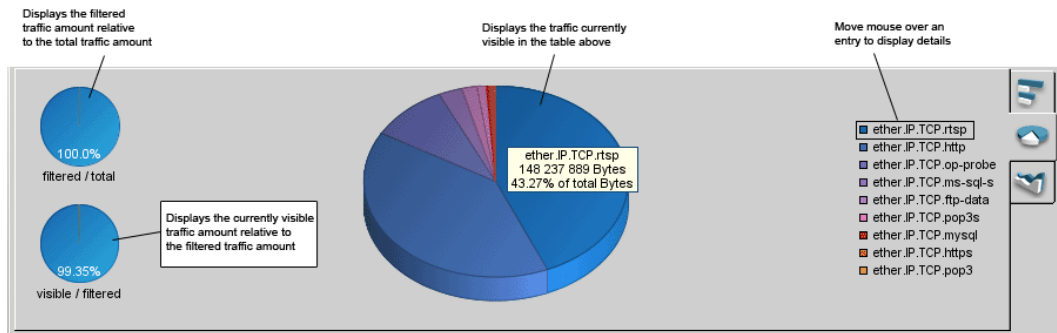
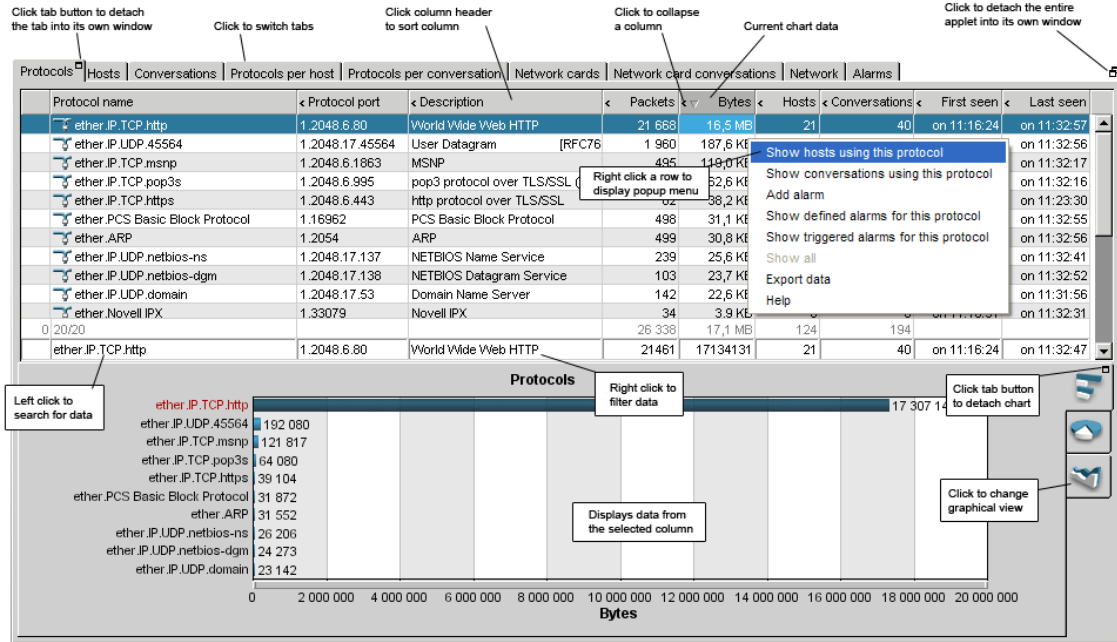
Chapter 4. Traffic Statistics

Overview

The Traffic Statistics screen lets you access live data. Show the Traffic Statistics screen by selecting the 'Traffic Statistics' button on the top of the window.



Applet interface overview





Switching network traffic view

Left click each tab located at the top to change between the different network traffic statistics views.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	
1 ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	25 877	20,4 MB	79	155	to 12:05:23	
ether.IP.TCP.netbios-ssn	1.2048.6.139	NETBIOS Session Service	11 878	2,4 MB	2	2	to 12:00:10	

The hosts tab was clicked, and the view switched to the hosts table:

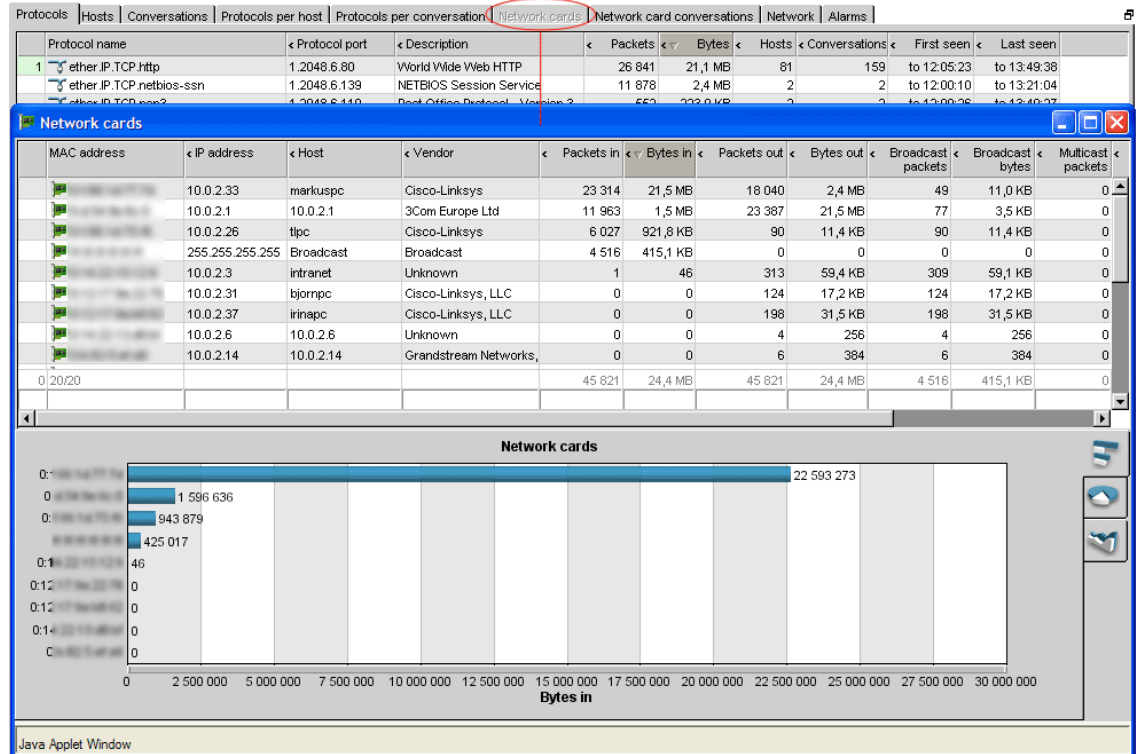
Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms	
Host name	Address	Packets in	Bytes in	Packets out	Bytes out	Mcast/bcast	Protocols	Conversations	First
 markuspc	10.0.2.33	19 622	17,7 MB	15 219	2,2 MB	27	6	158	tc
 tlpc	10.0.2.26	5 924	911,7 KB	5 843	1,5 MB	46	4	6	tc

Detaching a tab to a window



You can detach a tab into its own top-level window by doing a right-click on the tab, or clicking the tab detach button that appears when you move the mouse over the right edge of the tab. This enables you to see more than one type of network statistics at the same time as well as giving you the possibility to resize the window.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms			
	MAC address	IP address	Host	Vendor	Packets in	Bytes in	Packets out	Bytes out	Broadcast packets	Broadcast bytes	Multicast packets
	0:f:66:1d:77:66	10.0.2.33	markuspc	Cisco-Linksys	23 165	21,5 MB	17 878	2,4 MB	43	9,7 KB	0
	0:d:54:9e:6c:54	10.0.2.1	10.0.2.1	3Com Europe Ltd	11 807	1,5 MB	23 234	21,5 MB	73	3,3 KB	0

The network cards tab was detached into its own top-level window, and resized to allow all the columns to be displayed at once.

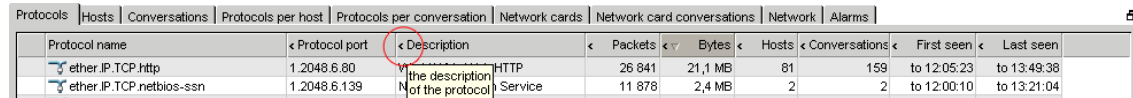


You can also click the detach button located at the top right to detach the entire main application window. This enables you to resize the application while at the same time having all the views inside one window frame.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms		
MAC address	IP address	Host	Vendor	Packets in	Bytes in	Packets out	Bytes out	Broadcast packets	Broadcast bytes	Multicast packets
 0:f:66:1d:77:66	10.0.2.33	markuspc	Cisco-Linksys	23 417	21,6 MB	18 143	2,4 MB	50	11,3 KB	0
 0:d:54:9e:6c:54	10.0.2.1	10.0.2.1	3Com Europe Ltd	12 065	1,5 MB	23 495	21,6 MB	82	3,7 KB	0



Collapsing and resizing a table column

A table's column can be resized by dragging the edge of the desired column header or collapsed entirely by clicking the little left arrow in the column header.



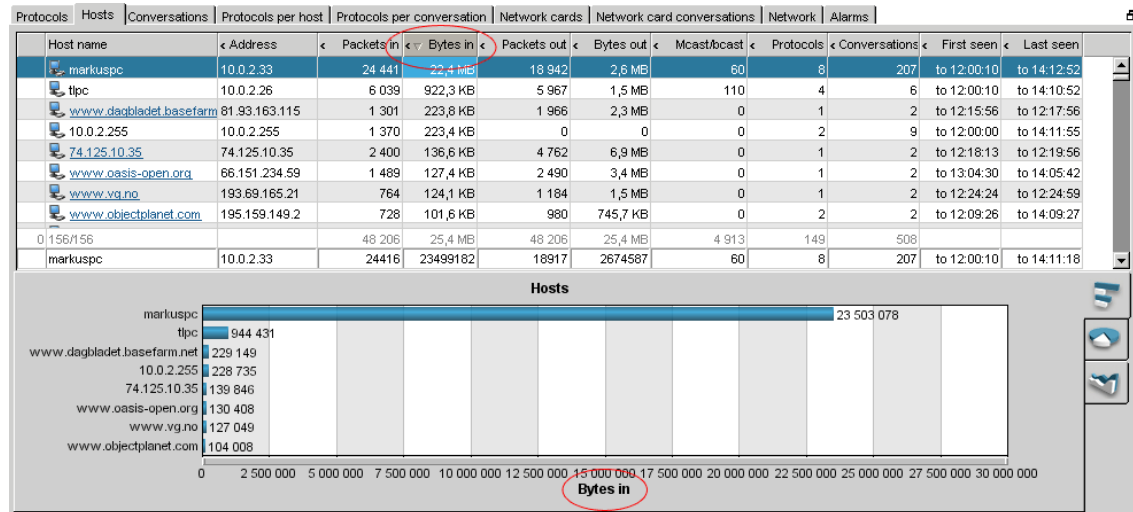
Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	Last seen
ether.IP.TCP.http	1.2048.6.80	the description of the protocol	26 841	21,1 MB	81	159	to 12:05:23	to 13:49:38
ether.IP.TCP.netbios-ssn	1.2048.6.139		11 878	2,4 MB	2	2	to 12:00:10	to 13:21:04

A column is made visible again by clicking the same arrow, now pointing to the right in the collapsed column header.

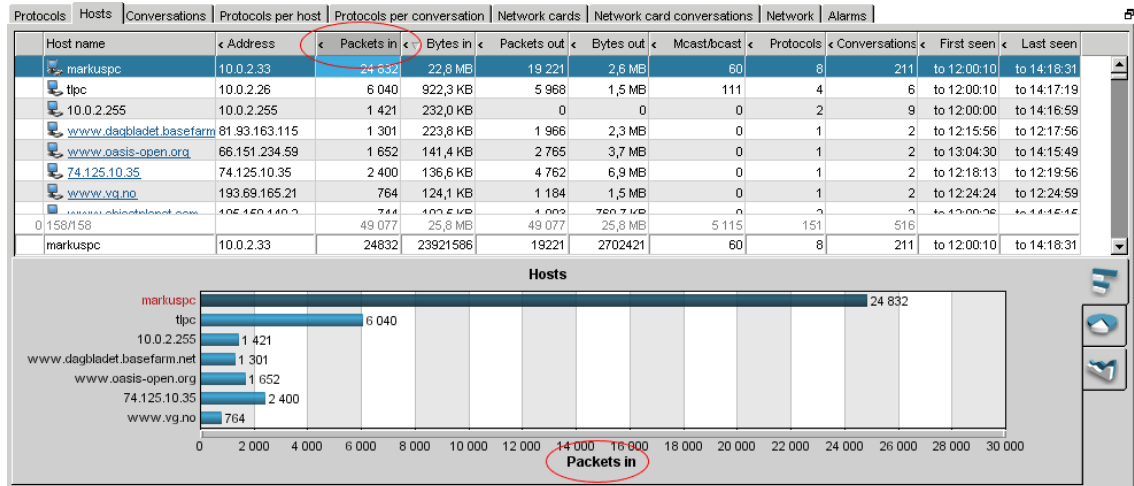
Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Protocol name	Protocol port	>< Packets	Bytes	Hosts	Conversations	First seen	Last seen	
 ether.IP.TCP.http	1.2048.6.80	the description of the protocol	21,1 MB	81	159	to 12:05:23	to 13:49:38	
 ether.IP.TCP.netbios-ssn	1.2048.6.139		2,4 MB	2	2	to 12:00:10	to 13:21:04	

Changing the data in the charts

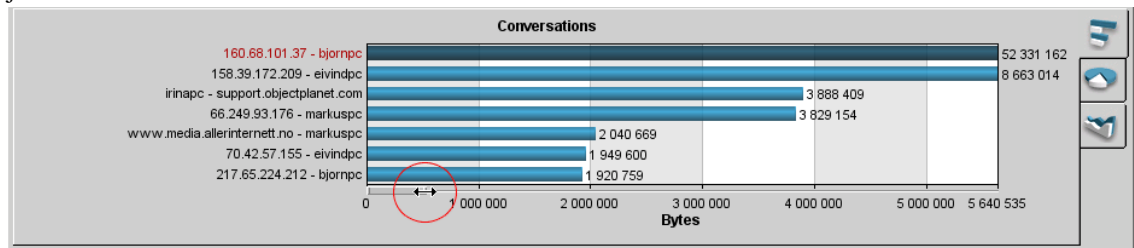
The data displayed in the bar chart and pie chart is the amount from the currently selected column, indicated with a slightly darker column header background.



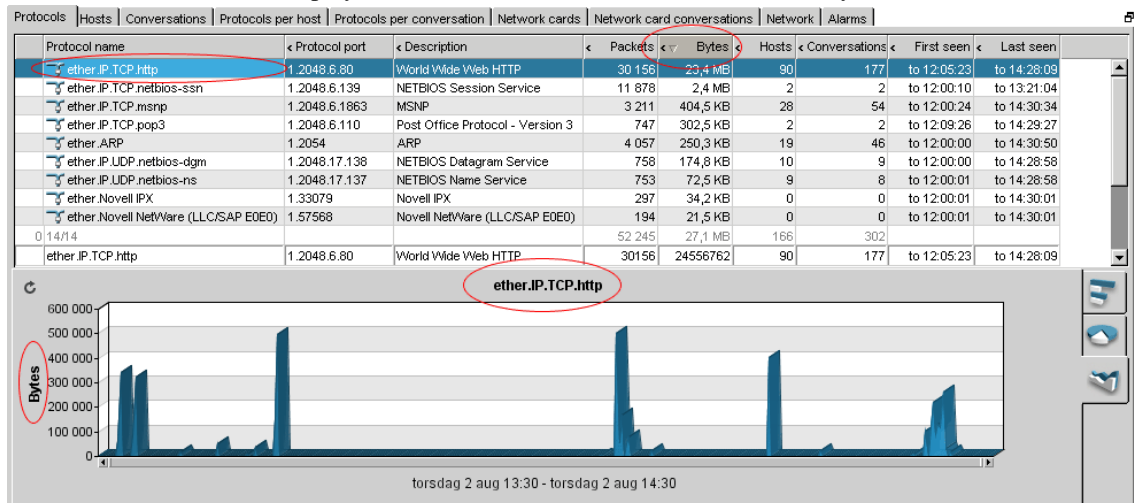
The data can be changed by selecting a cell from another column. Only data from numerical columns can be visualized in the bar chart. You can also change the selected column by typing the left or right key on your keyboard.



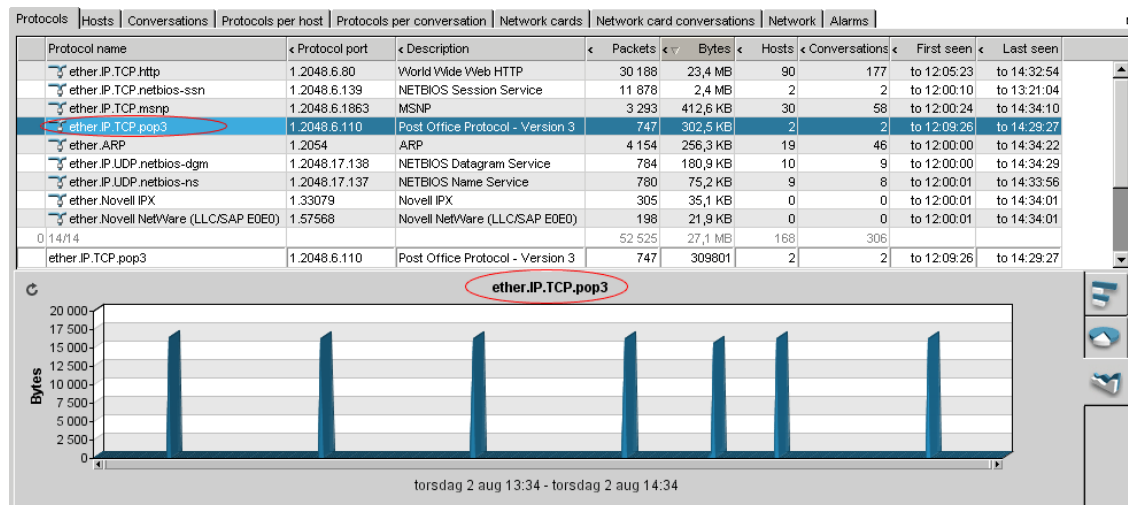
The range of the chart can be adjusted by dragging the range adjuster placed at the bottom of the chart, just above the axis values.



The data in the line chart displays the traffic amount over time for the currently selected row and cell.



Change the data in the line chart by selecting another row in the table.



Sorting a table column

Left click a table's column header to sort the selected column. Textual columns are sorted in ascending order while numerical columns are sorted in descending order with the largest value at the top. Click the column header again to sort in the opposite order.

Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	Last seen
ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	44 723	34,1 MB	120	237	to 12:05:23	to 14:48:17
ether.IP.TCP.netbios-ssn	1.2048.6.139	NETBIOS Session Service	11 878	2,4 MB	2	2	to 12:00:10	to 13:21:04
ether.ARP	1.2054	ARP	4 602	284,0 KB	19	46	to 12:00:00	to 14:48:12
ether.IP.TCP.msnp	1.2048.6.1863	MSNP	3 539	438,2 KB	34	66	to 12:00:24	to 14:48:56
ether.IP.UDP.netbios-dgm	1.2048.17.138	NETBIOS Datagram Service	880	202,9 KB	10	9	to 12:00:00	to 14:48:22
ether.IP.UDP.netbios-ns	1.2048.17.137	NETBIOS Name Service	866	83,4 KB	9	8	to 12:00:01	to 14:47:23
ether.IP.TCP.pop3	1.2048.6.110	Post Office Protocol - Version 3	787	318,5 KB	2	2	to 12:09:26	to 14:39:28
ether.Novell IPX	1.33079	Novell IPX	335	38,6 KB	0	0	to 12:00:01	to 14:48:02

The currently sorted column will have a sort order indicator visible in the column header, indicating which order the column was sorted in.

Searching for network traffic details

The fields at the bottom of each table is called the filter bar and can be used to search for network traffic details. Left click one of the fields in the filter bar to start typing. As you type, the first row matching the text in the respective column is automatically scrolled to and selected in the table.

Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	Last seen
ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	44 745	34,1 MB	121	239	to 12:05:23	to 14:49:55
ether.IP.TCP.netbios-ssn	1.2048.6.139	NETBIOS Session Service	11 878	2,4 MB	2	2	to 12:00:10	to 13:21:04
ether.ARP	1.2054	ARP	4 602	284,0 KB	19	46	to 12:00:00	to 14:51:12
ether.IP.TCP.msnp	1.2048.6.1863	MSNP	3 552	439,0 KB	34	66	to 12:00:24	to 14:50:38
ether.IP.UDP.netbios-dgm	1.2048.17.138	NETBIOS Datagram Service	881	203,1 KB	10	9	to 12:00:00	to 14:49:50
ether.IP.UDP.netbios-ns	1.2048.17.137	NETBIOS Name Service	866	83,4 KB	9	8	to 12:00:01	to 14:47:23
ether.IP.TCP.pop3	1.2048.6.110	Post Office Protocol - Version 3	826	334,4 KB	2	2	to 12:09:26	to 14:49:27
ether.Novell IPX	1.33079	Novell IPX	339	39,1 KB	0	0	to 12:00:01	to 14:51:02
ether.Novell NetWare (LLC/SAP E0E0)	1.57568	Novell NetWare (LLC/SAP E0E0)	221	24,5 KB	0	0	to 12:00:01	to 14:51:02

The phrase 'pop3' was typed in the first field of the filter bar, and the ether.IP.TCP.pop3 protocol was found in the table.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	Last seen
ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	44 748	34,1 MB	121	239	to 12:05:23	to 14:53:27
ether.IP.TCP.netbios-ssn	1.2048.6.139	NETBIOS Session Service	11 878	2,4 MB	2	2	to 12:00:10	to 13:21:04
ether.ARP	1.2054	ARP	4 682	288,9 KB	19	46	to 12:00:00	to 14:54:02
ether.IP.TCP.msnpp	1.2048.6.1863	MSNP	3 568	441,1 KB	34	66	to 12:00:24	to 14:53:38
ether.IP.UDP.netbios-dgm	1.2048.17.138	NETBIOS Datagram Service	892	205,7 KB	10	9	to 12:00:00	to 14:53:42
ether.IP.UDP.netbios-ns	1.2048.17.137	NETBIOS Name Service	880	84,8 KB	9	8	to 12:00:01	to 14:52:54
ether.IP.TCP.pop3	1.2048.6.110	Post Office Protocol - Version 3	826	334,4 KB	2	2	to 12:09:26	to 14:49:27
ether.Novell.IPX	1.33079	Novell IPX	345	39,8 KB	0	0	to 12:00:01	to 14:54:02
ether.Novell.NetWare (LLC/SAP E0E0)	1.57568	Novell NetWare (LLC/SAP E0E0)	226	25,0 KB	0	0	to 12:00:01	to 14:54:02
0/15/15			68 383	38,0 MB	208	384		
pop3								

For textual columns, a match is made if the row contains the text from the filter field in the column (substring). If you want an exact match, simply add an equals sign (=) in after the search text.

Filtering network traffic details

The fields at the bottom of each table is called the filter bar and can be used to filter out the actual network traffic details you are looking for. Right click one of the fields in the filter bar to display only those rows that include the text from the filter field in the respective column. You can filter multiple columns at the same time by right clicking another filter bar field.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Host name	Address	Protocol	Packets in	Bytes in	Packets out	Bytes out	First seen	Last seen
markuspc	10.0.2.33	ether.IP.TCP.http	27 000	31,9 MB	18 244	2,6 MB	to 12:05:23	to 14:57:05
www.dagbladet.basefarm.net	81.93.163.115	ether.IP.TCP.http	2 162	362,4 KB	3 336	3,9 MB	to 12:15:56	to 14:46:12
www.vg.no	193.69.165.21	ether.IP.TCP.http	1 522	234,3 KB	2 367	3,0 MB	to 12:24:24	to 14:45:38
www.oasis-open.org	66.151.234.59	ether.IP.TCP.http	1 979	169,4 KB	3 315	4,5 MB	to 13:04:30	to 14:56:54
74.125.10.35	74.125.10.35	ether.IP.TCP.http	2 400	136,6 KB	4 762	6,9 MB	to 12:18:13	to 12:19:56
track.adform.net	81.7.166.249	ether.IP.TCP.http	514	130,5 KB	583	600,1 KB	to 12:14:21	to 14:46:03
db-admatch.osl.basefarm.net	81.93.163.121	ether.IP.TCP.http	524	124,7 KB	788	943,3 KB	to 12:15:57	to 14:46:10
www.itavisen.no	82.117.42.52	ether.IP.TCP.http	372	98,5 KB	539	642,0 KB	to 12:14:49	to 12:16:12
0/155/253			45 400	34,6 MB	45 400	34,6 MB		
markuspc	10.0.2.33	ether.IP.TCP.http	18175	22863405	11977	1693117	to 12:05:23	to 14:27:54

In the above image the user selected a row with the www-http protocol and right clicked the filter bar field for the protocol column to display only hosts that have used the http protocol since the probe started or was reset.

Table 4.1. Filter operators

operator	description
filter	displays rows including the text 'filter'
filter=	displays rows exactly matching the text 'filter'
filter<>	displays rows not matching the text 'filter'
filter!*	displays rows not including the text 'filter'
filter>	displays rows including text or numbers larger than or equal to 'filter'
filter<	displays rows including text or numbers smaller than 'filter'
filter<=	displays rows including text or numbers smaller than or equal to 'filter'
filter & filter2 & ...	displays rows matching the filters (AND filter)
filter filter2 ...	displays rows matching the filters (OR filter)

In the below image the user typed in the filter <50 and right clicked the filter field (you can also type enter) to display protocols where the probe have seen less than 50 packets go by since it started or was reset. As this example illustrates, the filter operators can also be placed in front of the filter value.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	Last seen
ether.IP.TCP.http-alt	1.2048.6.8080	HTTP Alternate (see port 80)	10	1,4 KB	2	2	to 14:42:15	to 14:42:15
ether.802.LANMAN.Standards.Commit	1.34958	802 LANMAN Standards Commit	6	798	0	0	to 12:48:40	to 14:49:14
ether.IP.ICMP	1.2048.1	Internet Control Message	3	222	2	1	to 13:36:25	to 13:36:28
ether.IP.UDP.bootpc	1.2048.17.68	Bootstrap Protocol Client	1	594	2	1	to 14:12:51	to 14:12:51
0/4/15			20	3,0 KB	6	4		
ether.IP.TCP.http-alt	1.2048.6.8080	HTTP Alternate (see port 80)	<50	1419	2	2	to 14:42:15	to 14:42:15

Viewing more detail

By right clicking a table row a popup menu is displayed giving you the opportunity to zoom into more details about the selected entry.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Protocol name	Protocol port	Description	Packets	Bytes	Hosts	Conversations	First seen	Last seen
ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	45 686	34,9 MB	121	239	to 12:05:23	to 15:05:33
ether.IP.TCP.netbios-ssn	1.2048.6.139	NETBIOS Session Service				2	to 12:00:10	to 13:21:04
ether.ARP	1.2054	ARP				49	to 12:00:00	to 15:07:30
ether.IP.TCP.msnp	1.2048.6.1863	MSNP				70	to 12:00:24	to 15:06:51
ether.IP.UDP.netbios-dgm	1.2048.17.138	NETBIOS Datagram Service				9	to 12:00:00	to 15:07:28
ether.IP.UDP.netbios-ns	1.2048.17.137	NETBIOS Name Service				8	to 12:00:01	to 15:07:21
ether.IP.TCP.pop3	1.2048.6.110	Post Office Protocol - Version				2	to 12:09:26	to 14:59:28
ether.Novell.IPX	1.33079	Novell IPX				0	to 12:00:01	to 15:07:02
ether.Novell.NetWare (LLC/SAP E0ED)	1.57568	Novell NetWare (LLC/SAP E0E				0	to 12:00:01	to 15:07:02
0/15/15						393		
ether.IP.TCP.http	1.2048.6.80	World Wide Web HTTP	45686	36588802	121	239	to 12:05:23	to 15:05:33

If you choose the 'Show conversations using this protocol' in the popup above, the view will be switched to the protocols per conversation tab and the protocol filter will be set to display only http entries.

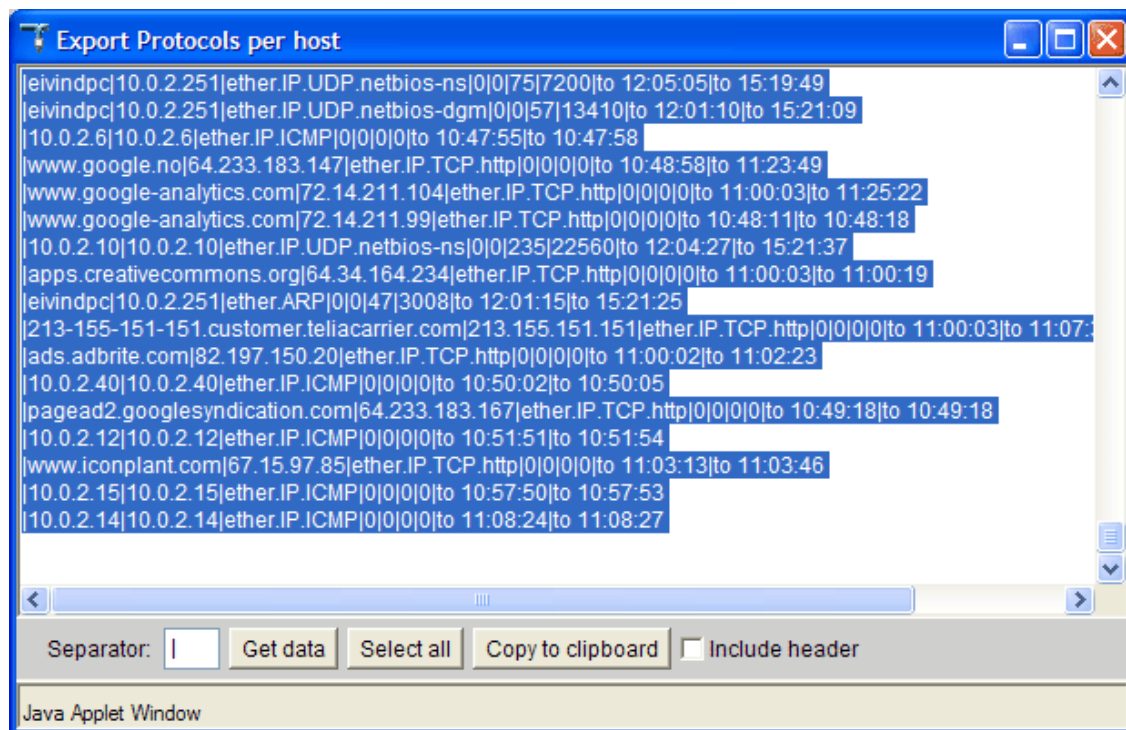
Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Source host	Destination host	Protocol	Packets	Bytes	First seen	Last seen		
74.125.10.35	markuspc	ether.IP.TCP.http	4 762	6,9 MB	to 12:18:13	to 12:19:56		
www.oasis-open.org	markuspc	ether.IP.TCP.http	3 591	4,9 MB	to 13:04:30	to 15:05:29		
www.dagbladet.basefarm	markuspc	ether.IP.TCP.http	3 338	3,9 MB	to 12:15:56	to 14:46:12		
www.vg.no	markuspc	ether.IP.TCP.http	2 367	3,0 MB	to 12:24:24	to 14:42:25		
kampanje.filmweb.no	markuspc	ether.IP.TCP.http	1 009	1,4 MB	to 14:39:47	to 14:42:04		
go.vg.no	markuspc	ether.IP.TCP.http	802	1 005,1 KB	to 12:24:25	to 14:42:13		
annonser.dagbladet.no	markuspc	ether.IP.TCP.http	788	943,3 KB	to 12:15:57	to 14:46:10		
www.sport1.de	markuspc	ether.IP.TCP.http	936	915,4 KB	to 12:14:29	to 14:39:38		
0/311/486			46 333	35,2 MB				
		ether.IP.TCP.http=						

Exporting network traffic data

By right clicking in the network traffic table you want to export data from, a popup with an 'Export data' choice will be displayed.

Protocols	Hosts	Conversations	Protocols per host	Protocols per conversation	Network cards	Network card conversations	Network	Alarms
Host name	Address	Protocol	Packets in	Bytes in	Packets out	Bytes out	First seen	Last seen
markuspc	10.0.2.33	ether.IP.TCP.http	28 017	33,0 MB	19 113	2,9 MB	to 12:05:23	to 15:21:12
markuspc	10.0.2.33	ether.IP.TCP.netbios-				921,5 KB	to 12:00:10	to 13:21:04
tpc	10.0.2.26	ether.IP.TCP.netbios-				1,5 MB	to 12:00:10	to 13:21:04
www.dagbladet.basefarm.net	61.93.163.115	ether.IP.TCP.http				3,9 MB	to 12:15:56	to 14:46:12
markuspc	10.0.2.33	ether.IP.TCP.pop3				23,7 KB	to 12:09:26	to 15:19:28
markuspc	10.0.2.33	ether.IP.TCP.msnp				188,4 KB	to 12:00:24	to 15:21:32
10.0.2.255	10.0.2.255	ether.IP.UDP.netbios-				0	to 12:00:00	to 15:21:09
www.vg.no	193.69.165.21	ether.IP.TCP.http				3,0 MB	to 12:24:24	to 14:45:38
0/268/268						39,8 MB		
markuspc	10.0.2.33	ether.IP.TCP.http				2903540	to 12:05:23	to 15:16:57
0/311/486						34 554 948		

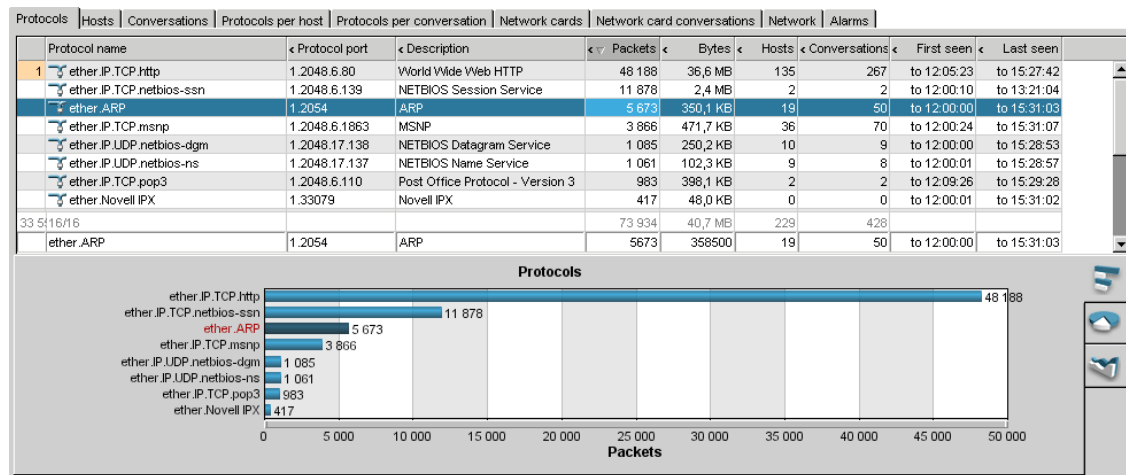
When you select 'Export data' a window is opened containing all the data in the table in a text area which you can use to copy and paste the data. The data in the window is exactly the same data as in the table with the correct sorting, filter settings, and visible columns.



You can change the field separator by typing it into the text field available for this and clicking the 'Get data' button. The header fields can also be included by turning on the 'Include header' checkbox.

Protocols

The protocols tab displays information about the protocols discovered by the probe on the network segment since it started or was reset.

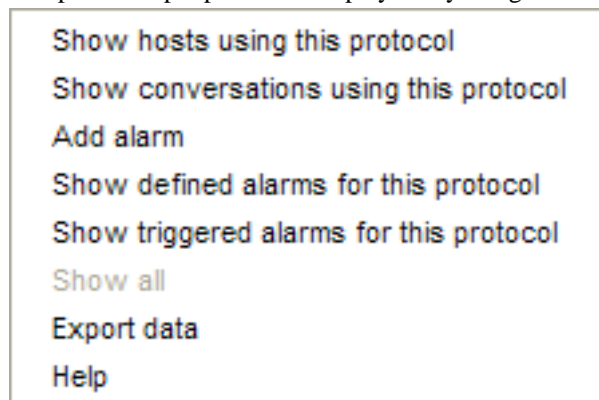


- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **protocol name** - the full name of the protocol. The name consists of the fully encapsulated name with the actual protocol being the last name. ether.IP.TCP.www-http is the HTTP protocol (web browsing) running on top of TCP running on top of IP running on top of Ethernet.

- **protocol port** - the protocol ID and port number for the protocol. The protocol port consists of the protocol numbers and ports for the encapsulating protocols and the actual protocol port being the last number. In the protocol ID 1.2048.6.80, 1 defines Ethernet, 2048 (0x0800) is IP, 6 is TCP and 80 is the HTTP port number.
- **description** - Describes the protocol in more detail.
- **packets** - the number of packets seen of each protocol on the network segment since the probe started or was reset.
- **bytes** - the number of bytes seen of each protocol on the network segment since the probe started or was reset.
- **hosts** - the number of hosts that have used this protocol since the probe started or was reset.
- **conversations** - the number of conversations that have used this protocol since the probe started or was reset.
- **first seen** - the time when the network probe first discovered each protocol on the network segment after the probe started or was reset.
- **last seen** - the time when the network probe last saw each protocol on the network segment after the probe started or was reset.

Protocols popup menu

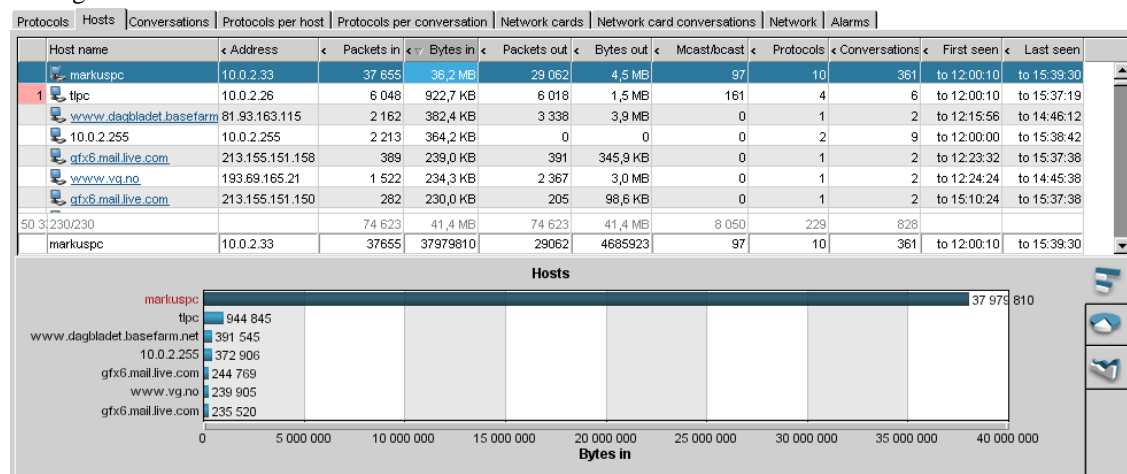
The protocols popup menu is displayed if you right click a protocol entry.



- **Show hosts using this protocol** - this will display all the host entries that have sent or received data using the selected protocol since the probe started or was reset. The protocols per host tab will be displayed.
- **Show conversations using this protocol** - this will display all the conversation entries that have used the selected protocol since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Add alarm** - this will let you add an alarm for this protocol. The add alarm window will be displayed.
- **Show defined alarms for this protocol** - this will display all the defined alarms for this protocol. The alarms tab will be displayed.
- **Show triggered alarms for this protocol** - this will display all the triggered alarms for this protocol. The alarms tab will be displayed.

Hosts

The hosts tab displays information about the hosts that have sent or received data on the network segment since the probe started or was reset. The hosts can be computers on the network segment or computers outside the network segment (such as the Internet) that have sent or received data with hosts on the segment.



- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **host name** - the name of the host as discovered by dns lookup.
- **address** - the IP address of the host.
- **packets in** - the number of packets received by each host since the probe started or was reset.
- **bytes in** - the amount of data received by each host since the probe started or was reset.
- **packets out** - the number of packets sent by each host since the probe started or was reset.
- **bytes out** - the amount of data sent by each host since the probe started or was reset.
- **mcast/bcast** - the number of broadcast or multicast packets sent by each host since the probe started or was reset.
- **protocols** - the number of protocols used by this host since the probe started or was reset.
- **conversations** - the number of conversations this host has participated in either as a source or destination since the probe started or was reset.
- **first seen** - the time when the network probe first discovered traffic from each host after the probe started or was reset.
- **last seen** - the time when the network probe last saw traffic from each host after the probe started or was reset.

Hosts popup menu

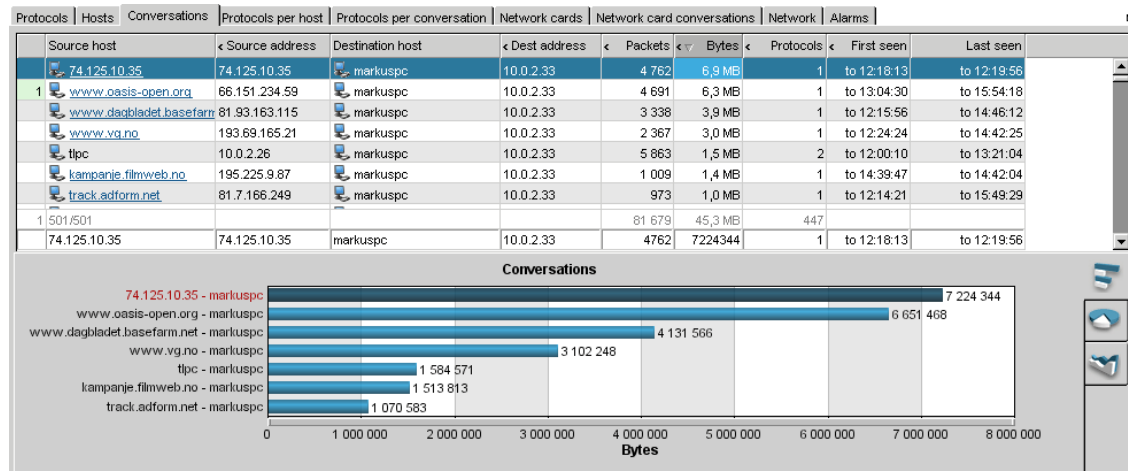
The hosts popup menu is displayed if you right click a host entry.

Show protocols used by this host
Show source conversations for this host
Show destination conversations for this host
Show source conversations and protocols for this host
Show destination conversations and protocols for this host
Add alarm
Show defined alarms for this host
Show triggered alarms for this host
Show all
Export data
Help

- **Show protocols used by this host** - this will display all the protocols that have been used for sending or receiving data by the selected host since the probe started or was reset. The protocols per host tab will be displayed.
- **Show source conversations for this host** - this will display all the conversations where the selected host has been sending data since the probe started or was reset. The conversations tab will be displayed.
- **Show destination conversations for this host** - this will display all the conversations where the selected host has been receiving data since the probe started or was reset. The conversations tab will be displayed.
- **Show source conversations and protocols for this host** - this will display all the protocols used in the conversations the selected host has sent data since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Show destination conversations and protocols for this host** - this will display all the protocols used in the conversations the selected host has received data since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Add alarm** - this will let you add an alarm for this host. The add alarm window will be displayed.
- **Show defined alarms for this host** - this will display all the defined alarms for this host. The alarms tab will be displayed.
- **Show triggered alarms for this host** - this will display all the triggered alarms for this host. The alarms tab will be displayed.

Conversations

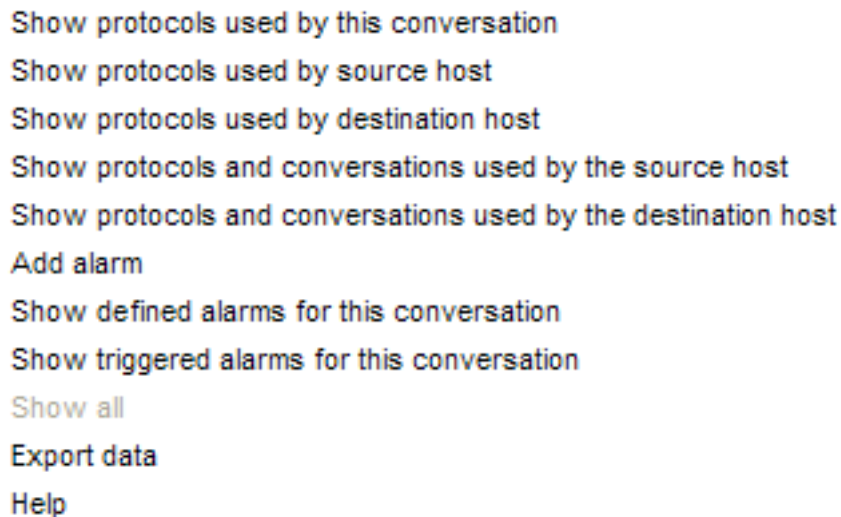
The conversations tab displays information about conversations that have taken place on the network segment since the probe started or was reset. The conversations can be from host to host on the network segment or to and from hosts outside the network segment such as the Internet.



- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **source host** - the name of the host sending the data in each conversation.
- **source address** - the IP address of the host sending the data in each conversation.
- **destination host** - the name of the host receiving the data in each conversation.
- **destination address** - the IP address of the host sending the data in each conversation.
- **packets** - the number of packets seen of each conversation on the network segment since the probe started or was reset.
- **bytes** - the number of bytes seen of each conversation on the network segment since the probe started or was reset.
- **protocols** - the number of protocols used by this conversation since the probe started or was reset.
- **first seen** - the time when the network probe first saw traffic for each conversation after the probe started or was reset.
- **last seen** - the time when the network probe last saw traffic for each conversation after the probe started or was reset.

Conversations popup menu

The conversations popup menu is displayed if you right click a conversation entry.

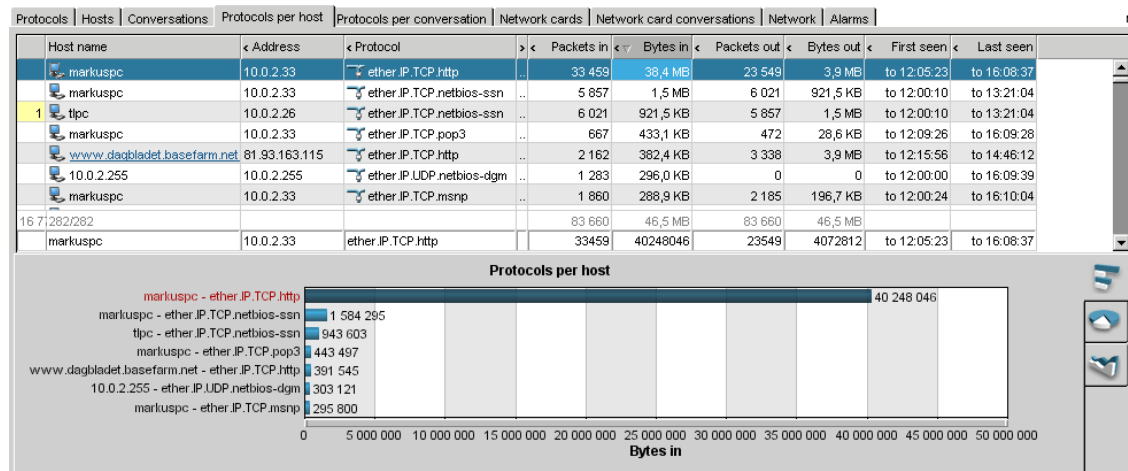


Show protocols used by this conversation
Show protocols used by source host
Show protocols used by destination host
Show protocols and conversations used by the source host
Show protocols and conversations used by the destination host
Add alarm
Show defined alarms for this conversation
Show triggered alarms for this conversation
Show all
Export data
Help

- **Show protocols used by this conversation** - this will display all the protocols that have been used in the selected conversation since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Show protocols used by source host** - this will display all the protocols used by the source host of the selected conversation since the probe started or was reset. The protocols per host tab will be displayed.
- **Show protocols used by destination host** - this will display all the protocols used by the destination host of the selected conversation since the probe started or was reset. The protocols per host tab will be displayed.
- **Show protocols and conversations used by the source host** - this will display all the protocols and conversations for the source host of the selected conversation since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Show protocols and conversations used by the destination host** - this will display all the protocols and conversations for the destination host of the selected conversation since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Add alarm** - this will let you add an alarm for this conversation. The add alarm window will be displayed.
- **Show defined alarms for this conversation** - this will display all the defined alarms for this conversation. The alarms tab will be displayed.
- **Show triggered alarms for this conversation** - this will display all the triggered alarms for this conversation. The alarms tab will be displayed.

Protocols per host

The protocols per host tab displays protocols used by each host discovered on the network segment and the amount of traffic sent or received for each of these protocols.



- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **host name** - the name of the host as discovered by dns lookup.
- **address** - the IP address of the host.
- **protocol** - the full name of the protocol. The name consists of the fully encapsulated name with the actual protocol being the last name. ether.IP.TCP.www-http is the HTTP protocol (web browsing) running on top of TCP running on top of IP running on top of Ethernet.
- **protocol port** - the protocol ID and port number for the protocol. The protocol port consists of the protocol numbers and ports for the encapsulating protocols and the actual protocol port being the last number. In the protocol ID 1.2048.6.80, 1 defines Ethernet, 2048 (0x0800) is IP, 6 is TCP and 80 is the HTTP port number. This column is collapsed.
- **packets in** - the number of packets of a specific protocol received by each host since the probe started or was reset.
- **bytes in** - the amount of data received of a specific protocol by each host since the probe started or was reset.
- **packets out** - the number of packets of a specific protocol sent by each host since the probe started or was reset.
- **bytes out** - the amount of data sent of a specific protocol by each host since the probe started or was reset.
- **first seen** - the time the network probe first discovered this type of traffic for a host after the probe started or was reset.
- **last seen** - the time the network probe last saw traffic of this type for a host after the probe started or was reset.

Protocols per host popup menu

The protocols per host popup menu is displayed if you right click an entry.

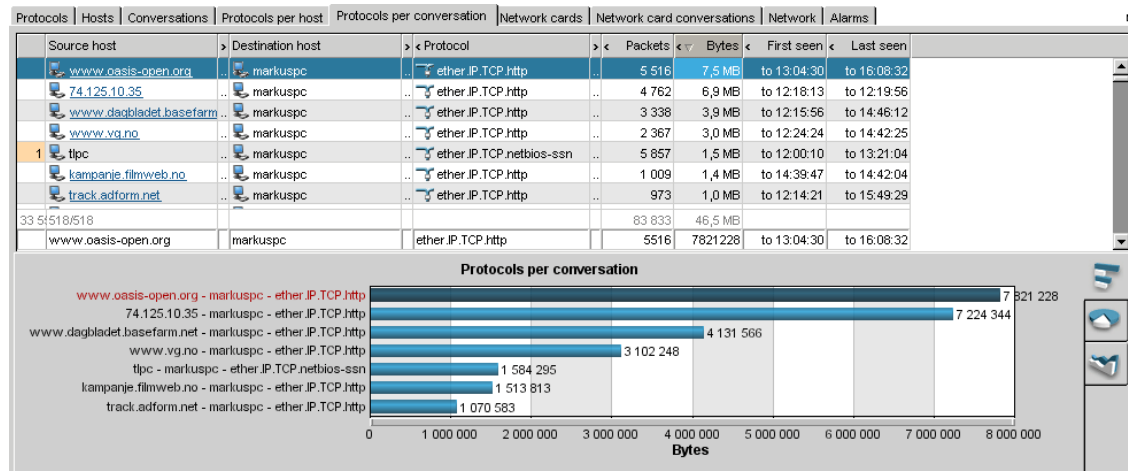
Show hosts using this protocol
Show conversations using this protocol
Show protocols used by this host
Show source conversations for this host
Show destination conversations for this host
Add alarm
Show defined alarms for this protocol and host
Show triggered alarms for this protocol and host
Show all
Export data
Help

- **Show hosts using this protocol** - this will display all the hosts that have sent or received data using the selected protocol since the probe started or was reset.
- **Show conversations using this protocol** - this will display all conversations seen using the selected protocol since the probe started or was reset. The protocols per conversation tab will be displayed.
- **Show protocols used by this host** - this will display the protocols that have been used for sending or receiving data by the selected host since the probe started or was reset.
- **Show source conversations for this host** - this will display all the conversations where the selected host have sent data since the probe started or was reset. The conversations tab will be displayed.
- **Show destination conversations for this host** - this will display all the conversations where the selected host have received data since the probe started or was reset. The conversations tab will be displayed.
- **Add alarm** - this will let you add an alarm for this protocol and host. The add alarm window will be displayed.
- **Show defined alarms for this protocol and host** - this will display all the defined alarms for this protocol and host. The alarms tab will be displayed.
- **Show triggered alarms for this protocol and host** - this will display all the triggered alarms for this protocol and host. The alarms tab will be displayed.

Protocols per conversation

The protocols per conversation tab displays the type of traffic used by each conversation discovered on the network segment and the amount of traffic sent or received for each of these protocols.

The links on the source and destination host entries indicate addresses where HTTP traffic has occurred. You can click on the links to open the address in a web page. Since the links only go to the root directory of the host, the page might not be valid or accessible.



- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **source host** - the name of the host sending the data as discovered by dns lookup.
- **source_address** - the IP address of the host sending the data. This column is hidden by default, click the arrow in the header to display the column.
- **destination host** - the name of the host receiving the data as discovered by dns lookup.
- **source_address** - the IP address of the host receiving the data. This column is hidden by default, click the arrow in the header to display the column.
- **protocol** - the full name of the protocol. The name consists of the fully encapsulated name with the actual protocol being the last name. ether.IP.TCP.www-http is the HTTP protocol (web browsing) running on top of TCP running on top of IP running on top of Ethernet.
- **protocol port** - the protocol ID and port number for the protocol. The protocol port consists of the protocol numbers and ports for the encapsulating protocols and the actual protocol port being the last number. In the protocol ID 1.2048.6.80, 1 defines Ethernet, 2048 (0x0800) is IP, 6 is TCP and 80 is the HTTP port number. This column is collapsed.
- **packets** - the number of packets seen of a specific protocol for each conversation on the network segment since the probe started or was reset.
- **bytes** - the amount of traffic seen of a specific protocol for each conversation on the network segment since the probe started or was reset.
- **first seen** - the time the network probe first discovered this type of traffic for a conversation after the probe started or was reset.
- **last seen** - the time the network probe last saw traffic of this type for a conversation after the probe started or was reset.

Protocols per conversation popup menu

The protocols per conversation popup menu is displayed if you right click an entry.

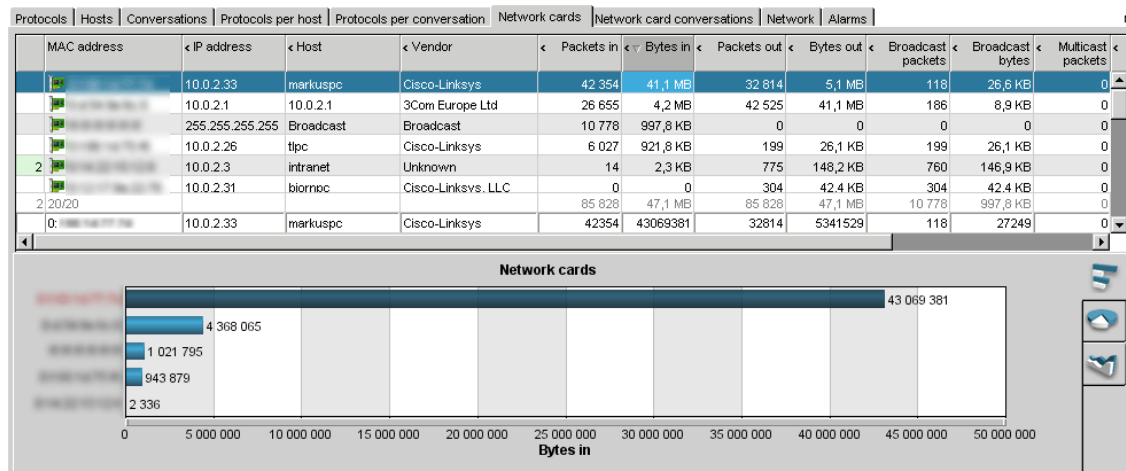
Show conversations using this protocol
Show hosts using this protocol
Show protocols used by this conversation
Show protocols used by source host
Show protocols used by destination host
Add alarm
Show defined alarms for this protocol and conversation
Show triggered alarms for this protocol and conversation
Show all
Export data
Help

- **Show conversations using this protocol** - this will display all conversations seen using the selected protocol since the probe started or was reset.
- **Show hosts using this protocol** - this will display all the hosts that have sent or received data using the selected protocol since the probe started or was reset. The protocols per host tab will be displayed.
- **Show protocols used by this conversation** - this will display all protocols used by the selected conversation since the probe started or was reset.
- **Show protocols used by source host** - this will display all protocols used by the source host of the selected conversation since the probe started or was reset. The protocols per host tab will be displayed.
- **Show protocols used by destination host** - this will display all protocols used by the destination host of the selected conversation since the probe started or was reset. The protocols per host tab will be displayed.
- **Add alarm** - this will let you add an alarm for this protocol and conversation. The add alarm window will be displayed.
- **Show defined alarms for this protocol and conversation** - this will display all the defined alarms for this protocol and conversation. The alarms tab will be displayed.
- **Show triggered alarms for this protocol and conversation** - this will display all the triggered alarms for this protocol and conversation. The alarms tab will be displayed.

Network cards

The network cards tab displays the network interfaces discovered and their traffic details. These network interfaces are physically connected to the same network segment as the probe is running on.

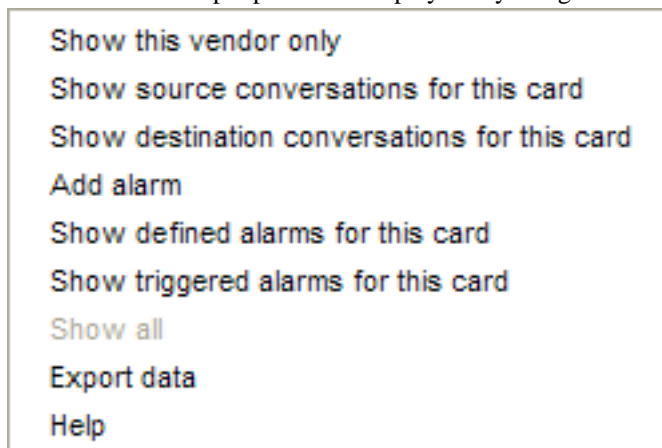
New network cards detected since the last reset are marked with a "new" icon.



- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **mac address** - the hardware address (MAC address) of the network card. Every network card in the world has a unique mac address. Network cards discovered for the first time will be marked with a red 'new' label in front of the address.
- **ip address** - the IP address of the host the network card sits in.
- **host** - the name of the host the network card sits in.
- **vendor** - the name of the vendor that manufactured the network card.
- **packets in** - the number of packets received by each network card since the probe started or was reset.
- **bytes in** - the amount of data received by each network card since the probe started or was reset.
- **packets out** - the number of packets sent by each network card since the probe started or was reset.
- **bytes out** - the amount of data sent by each network card since the probe started or was reset.
- **broadcast packets** - the number of broadcast packets sent by each network card since the probe started or was reset.
- **broadcast bytes** - the amount of broadcast data sent by each network card since the probe started or was reset.
- **broadcast packets** - the number of multicast packets sent by each network card since the probe started or was reset.
- **broadcast bytes** - the amount of multicast data sent by each network card since the probe started or was reset.
- **first seen** - the time when the network probe first discovered traffic from each network card after the probe started or was reset.
- **last seen** - the time when the network probe last saw traffic from each network card after the probe started or was reset.

Network cards popup menu

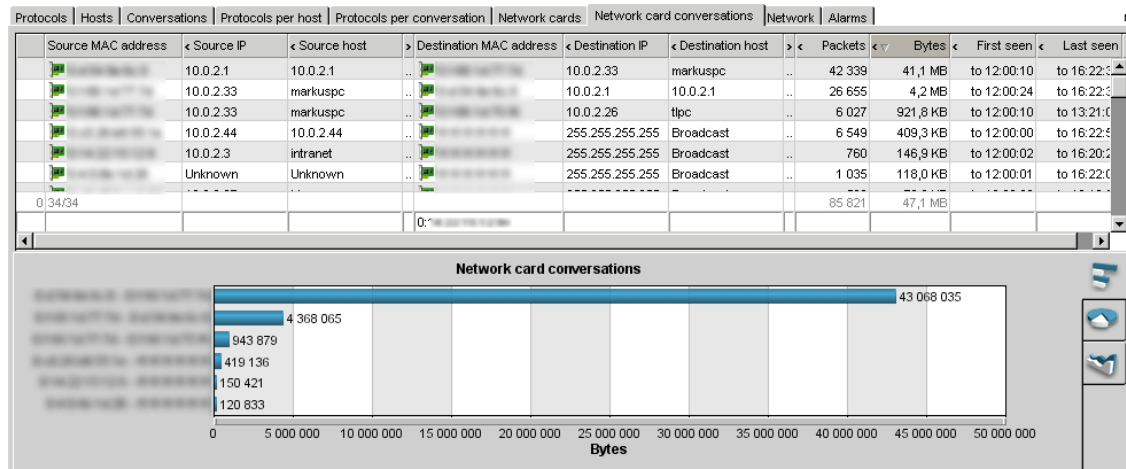
The network cards popup menu is displayed if you right click an entry.



- **Show this vendor only** - this will display all the network interfaces discovered on your network since the probe started or was reset and manufactured by the vendor in the selected interface.
- **Show source conversations for this card** - this will display all conversations among network cards where the selected card has sent data since the probe started or was reset. The network card conversations tab will be displayed.
- **Show destination conversations for this card** - this will display all conversations among network cards where the selected card has received data since the probe started or was reset. The network card conversations tab will be displayed.
- **Add alarm** - this will let you add an alarm for this network card. The add alarm window will be displayed.
- **Show defined alarms for this card** - this will display all the defined alarms for this network card. The alarms tab will be displayed.
- **Show triggered alarms for this card** - this will display all the triggered alarms for this network card. The alarms tab will be displayed.

Network card conversations

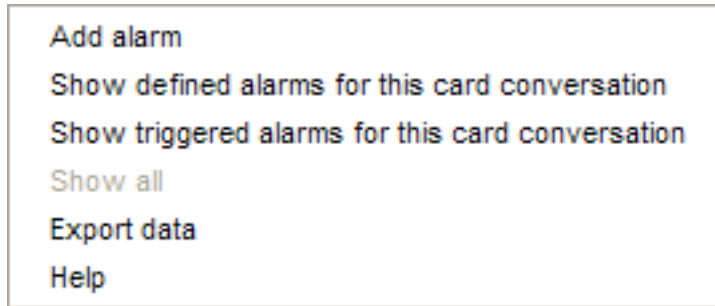
The network card conversations tab displays conversations discovered among the network interfaces connected to the network segment the probe is running on.



- **triggered alarm count** - the triggered alarm count for this entry color coded by the highest severity of the triggered alarms.
- **source address** - the hardware address (MAC address) of the network card sending data. Every network card in the world has a unique mac address.
- **source ip** - the IP address of the host sending data.
- **source host** - the name of the host sending data. This column is hidden and can be displayed by clicking the arrow in the column header.
- **source vendor** - the name of the vendor who manufactured the card sending data. This column is hidden and can be displayed by clicking the arrow in the column header.
- **destination address** - the hardware address (MAC address) of the network card receiving data. Every network card in the world has a unique mac address.
- **destination ip** - the IP address of the host receiving data.
- **destination host** - the name of the host receiving data. This column is hidden and can be displayed by clicking the arrow in the column header.
- **destination vendor** - the name of the vendor who manufactured the card receiving data. This column is hidden and can be displayed by clicking the arrow in the column header.
- **first seen** - the time when the network probe first discovered traffic between the network interfaces since the probe started or was reset.
- **last seen** - the time when the network probe last saw traffic between the network interfaces since the probe started or was reset.

Network card conversations popup menu

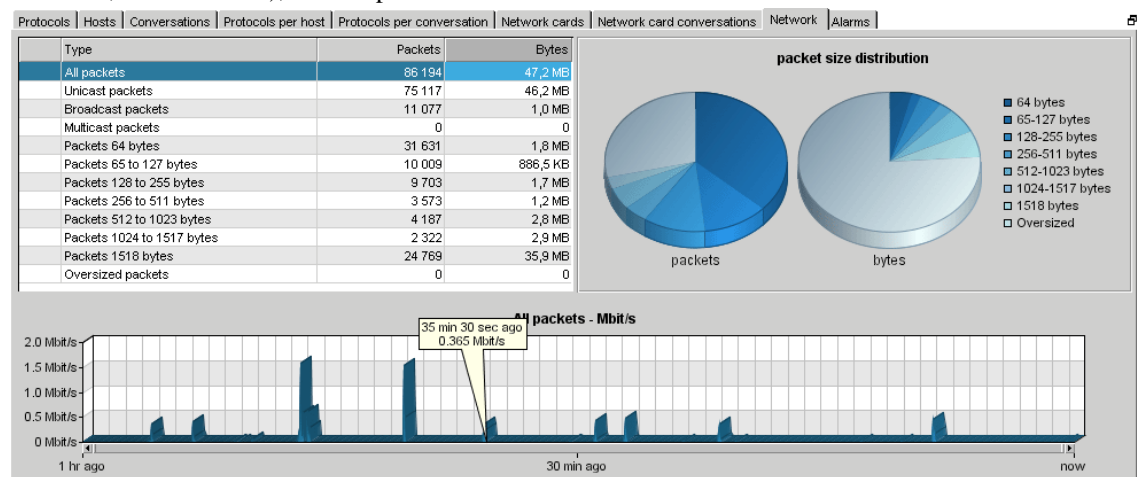
The network card conversations popup menu is displayed if you right click an entry.



- **Add alarm**- this will let you add a alarm for this entry.
- **Show defined alarms for this card conversation** - displays the defined alarms for the clicked network card conversation. The alarms tab will be displayed.
- **Show triggered alarms for this entry** - displays the triggered alarms for the clicked network card conversation. The alarms tab will be displayed.
- **Delete alarm** - deletes the clicked alarm entry.

Network

The network tab displays the total amount of traffic for all packets, the packet type distribution (unicast, multicast, and broadcast), and the packet size distribution.



- **packet size distribution** - displays the distribution of the packet size. Move the mouse cursor over the pie elements to display detailed info about the size distribution.
- **network throughput** - displays the network throughput in number of Kbit/s or Mbit/s up to the last interval period (default 2 hours). Move the mouse cursor across the chart to display the time and throughput at a specific time. The chart can be scrolled and zoomed.

Network popup menu

The network popup menu is displayed if you right click an entry.

Add alarm
 Show defined alarms for this entry
 Show triggered alarms for this entry
 Export data
 Help

- **Add alarm-** this will let you add a alarm for this entry.
- **Show defined alarms for this entry** - displays the defined alarms for this entry. The alarms tab will be displayed.
- **Show triggered alarms for this entry** - displays the triggered alarms for this entry. The alarms tab will be displayed.
- **Delete alarm** - deletes the clicked alarm entry.

Alarms

The alarms tab displays the defined and triggered alarms. Alarms can also be created, edited and deleted from this tab.

Protocols | Hosts | Conversations | Protocols per host | Protocols per conversation | Network cards | Network card conversations | Network | Alarms

Triggered alarms

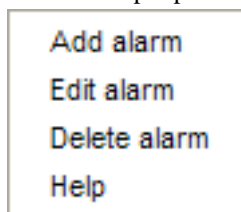
Trigger time	Count	Entry type	Entry	Field	Description
15.08.07 14:24:26	1	Protocol	ether.IP.TCP.http	Packets	
15.08.07 14:18:52	1	Protocol	ether.IP.TCP.msnp	Packets	
15.08.07 14:15:29	1	Protocol	ether.ARP	Packets	

- **Trigger time** - displays the time when the alarm was triggered
- **Count** - the trigger count for the alarm

- **Entry type** - the table the alarm is for.
- **Entry type** - the entry the alarm is for.
- **Field type** - the alarm is triggered based on this fields value.
- **Description** - the description set for the alarm.
- **Severity** - displaying the severity color coded.
- **Type** - the type of the alarm (Absolute, Delta).

Alarms popup menu

The alarms popup menu is displayed if you right click an alarm entry.

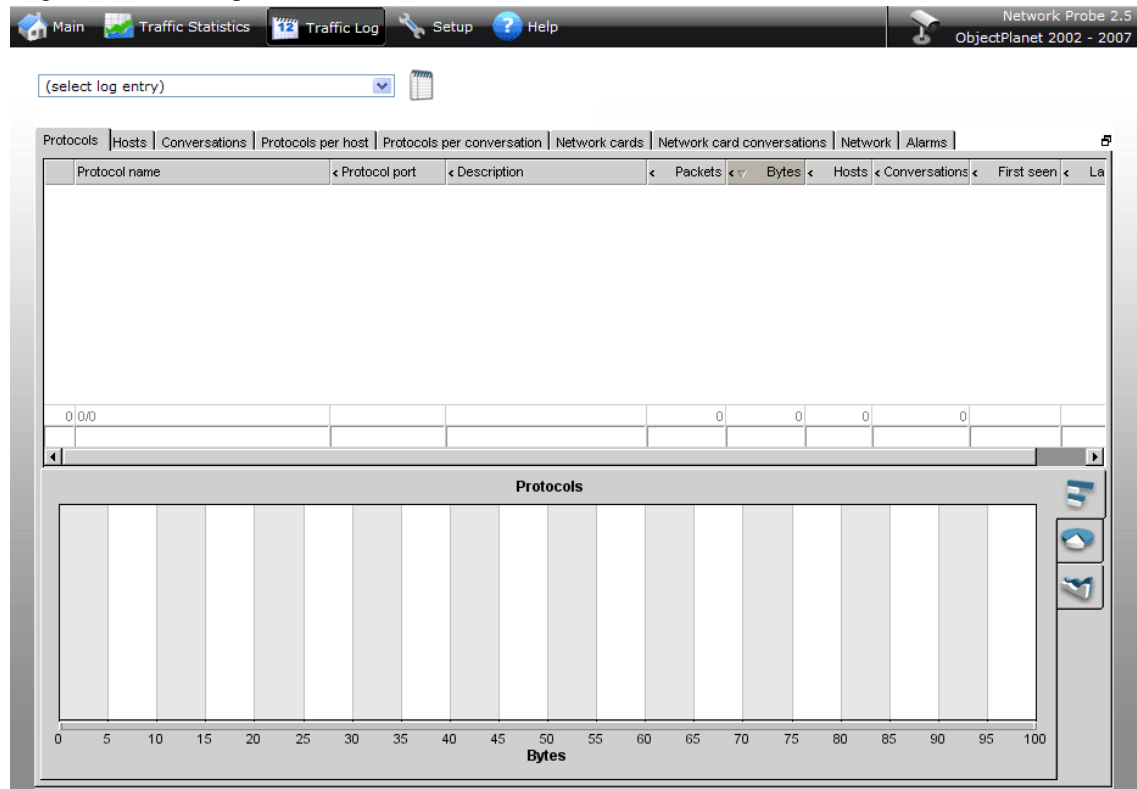


- **Add alarm**- this will let you add a alarm.
- **Edit alarm** - this will let you edit the clicked alarm. If the alarm clicked is a triggered alarm, the triggered alarms defined alarm will be changed.
- **Delete alarm** - deletes the clicked alarm entry.

Chapter 5. Traffic Log

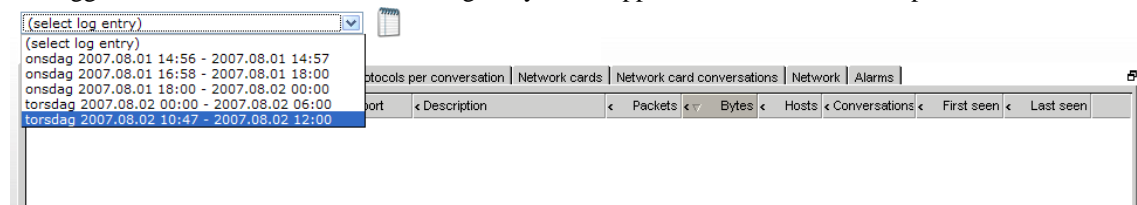
Overview

The Traffic Log screen lets you access saved data. When the probe is reset all the statistics data are saved to disk. By default this happens every 6th hour. Show the Traffic Log screen by selecting the 'Traffic Log' button on the top of the window.

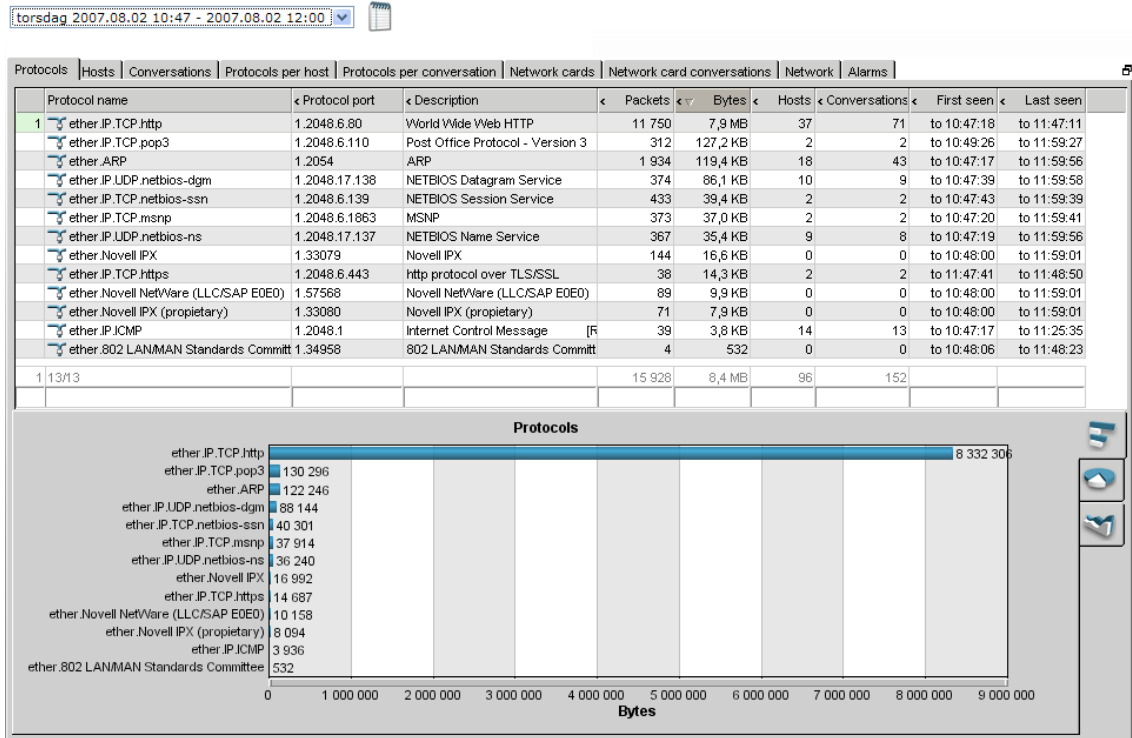


Display logged statistics

The Traffic Log screen shows the Network Probe applet with no data and a selection box with a list of all the logged network statistics. To view a log entry in the applet, select it from the drop down box.

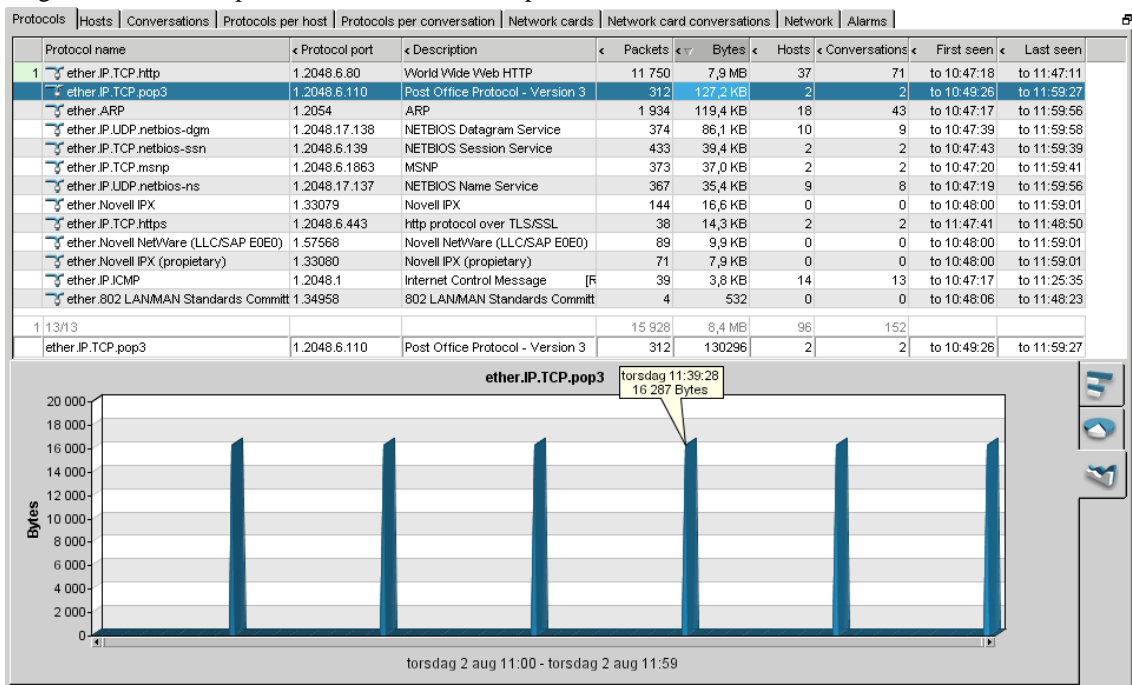


The network statistics from the selected time period will then be displayed in the network probe applet, and all the normal operations work as with the live data.



Logged interval data

The interval data displayed for the logged data might not match the period of the log selection, but is the length of the interval period set in the Probe setup.



The interval data displayed above covers 2 hours, same as the interval period set in the Statistics setup.

Set the duration of the interval data to the same as the reset interval to match the displayed interval data

with the log period selected.

The screenshot shows a window titled "Statistics" with a close button in the top right corner. The window is divided into two main sections. The top section, "Collected Statistics", has a "Set all" button and a table with three columns: "Collected Statistics", "Interval Duration", and "Interval Time". The bottom section, "Reset settings", displays the last and next reset times, the reset day, hour, and interval, along with "Update" and "Reset now" buttons.

Collected Statistics	Interval Duration	Interval Time
<input checked="" type="checkbox"/> Protocols	2 hours	Select a value
<input checked="" type="checkbox"/> Hosts	2 hours	10 seconds
<input checked="" type="checkbox"/> Conversations	2 hours	10 seconds
<input checked="" type="checkbox"/> Protocols per host	2 hours	10 seconds
<input checked="" type="checkbox"/> Protocols per conversation	2 hours	10 seconds
<input checked="" type="checkbox"/> Network cards	2 hours	10 seconds
<input checked="" type="checkbox"/> Network card conversations	2 hours	10 seconds
<input checked="" type="checkbox"/> Network overview	2 hours	10 seconds

Update

Reset settings

Last reset: 29. januar 2007 12:00
Next reset: 29. januar 2007 16:00
Reset day: Every day
Reset hour: Midnight
Reset interval: Every 2 hours
Update Reset now

Log manager



Display the log manager by selecting the Log Manager button above the log applet window. The log manager lists all the logged statistics entries, the amount of space used by the data, and the maximum allowed age of the entries in the database.

To limit the amount of data used by the logged statistics, you can automatically delete any entries older than the specified number of days. The default age is 30 days.

Clicking on a log entry will load that data in the log applet.

http://localhost:7030 - Log Manager - Mozilla Firefox

Size: 242.8 MB Delete entries older than days

Network Statistics Log	Age
Monday 2007.01.22 11:05 - 2007.01.22 12:00	7 days
Monday 2007.01.22 12:00 - 2007.01.22 17:59	7 days
Monday 2007.01.22 18:00 - 2007.01.23 00:00	7 days
Tuesday 2007.01.23 00:00 - 2007.01.23 06:00	6 days
Tuesday 2007.01.23 06:00 - 2007.01.23 12:00	6 days
Tuesday 2007.01.23 17:45 - 2007.01.23 17:59	6 days
Tuesday 2007.01.23 18:00 - 2007.01.23 23:59	6 days
Wednesday 2007.01.24 00:00 - 2007.01.24 05:59	5 days
Wednesday 2007.01.24 06:00 - 2007.01.24 12:00	5 days
Wednesday 2007.01.24 15:15 - 2007.01.24 17:06	5 days
Wednesday 2007.01.24 17:12 - 2007.01.24 17:23	5 days
Wednesday 2007.01.24 17:23 - 2007.01.24 18:00	5 days
Wednesday 2007.01.24 18:00 - 2007.01.25 00:00	5 days
Thursday 2007.01.25 00:00 - 2007.01.25 06:00	4 days
Thursday 2007.01.25 11:09 - 2007.01.25 11:59	4 days
Thursday 2007.01.25 14:22 - 2007.01.25 18:00	4 days
Thursday 2007.01.25 18:00 - 2007.01.25 23:59	4 days
Friday 2007.01.26 00:00 - 2007.01.26 06:00	3 days
Friday 2007.01.26 06:00 - 2007.01.26 12:00	3 days

Done

Chapter 6. Alarms

Alarms

Alarms can be added, removed and edited from both the "Traffic Statistics" and the "Main" tab. Triggered alarms are treated as statistics data. This means they are stored when the probe is reset, and can later on be viewed in the "Traffic Log" tab. When the probe is stopped triggered alarms are lost. Defined alarms are not affected by resetting or stopping the probe, they exist until they are deleted by the user. There exists two types of alarms: absolute alarms, and delta alarms.

Absolute alarms

An absolute alarm will be triggered when the monitored entries value for the given field increases over a specified trigger value. Once the alarm is triggered it will not trigger again until the probe is reset.

Delta alarms

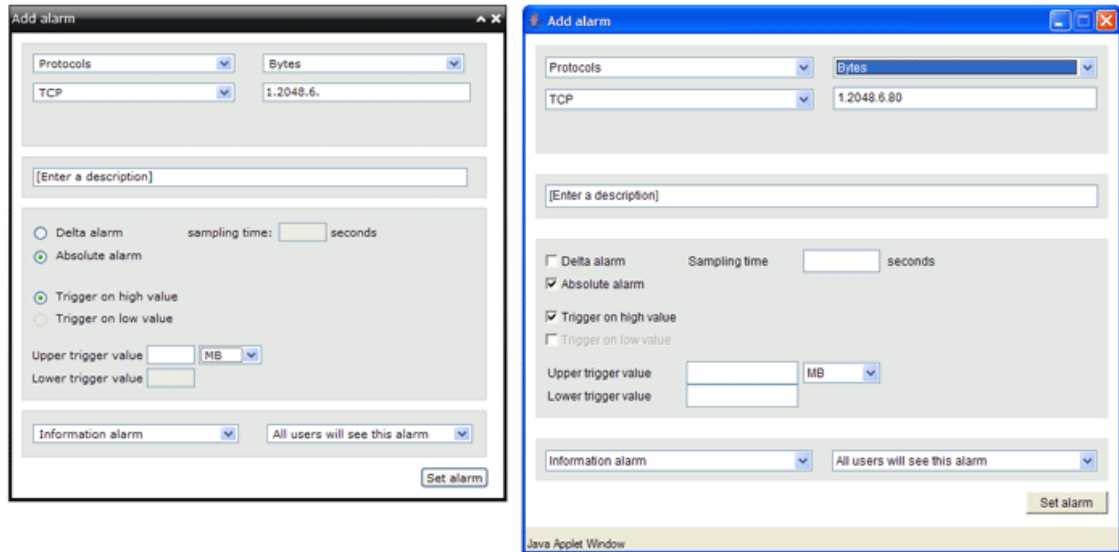
A delta alarm is triggered when the monitored entries delta value for the given field is larger than a specified value. For each sampling time there is taken a sample of the monitored entries value for the given field. If the difference of the two last samples taken is larger than the specified trigger value for a upper trigger type alarm, or lower than the specified trigger value for a lower trigger type alarm, the alarm is triggered.

Delta alarms can have upper or lower trigger type. A delta alarm with trigger type upper is triggered when the monitored entries delta value for the given field is larger than the specified trigger value. Once triggered, the alarm will not be triggered again if there is no lower trigger value set. Set a lower trigger value also to reset the alarm when the monitored entries delta value for the given field is smaller than the lower trigger value. If this happens, the alarm can be triggered again.

A delta alarm with trigger type lower is triggered when the monitored entries delta value for the given field is smaller than the specified lower trigger value. If an upper trigger value is set also the alarm can be triggered multiple times. If the monitored entries delta value for the given field is larger than the specified upper trigger value the alarm can be triggered again.

Adding alarms

In the "Main" screen, an alarm can be added by right clicking on an entry in the tables or choosing "New Alarm" in the Alarms top menu. In the "Traffic Statistics" tab, an alarm can be added by right clicking and choosing "Add alarm".



Entry

To add an alarm you first need to enter the entry you want the alarm to be for. You need to select the table and the field for the entry. Additionally you need to enter the entry. The below image shows adding an alarm for a Protocols per conversation entry on the Byte field. The entry to add the alarm for is between hosts 10.0.2.3 and 10.0.2.4, using protocol 1.2048.6.80 (TCP port 80).

Protocols per conversation	Bytes
TCP	1.2048.6.80
10.0.2.3	10.0.2.4

Description

Optionally you can add a description for the alarm.

[Enter a description]

Alarm and trigger type

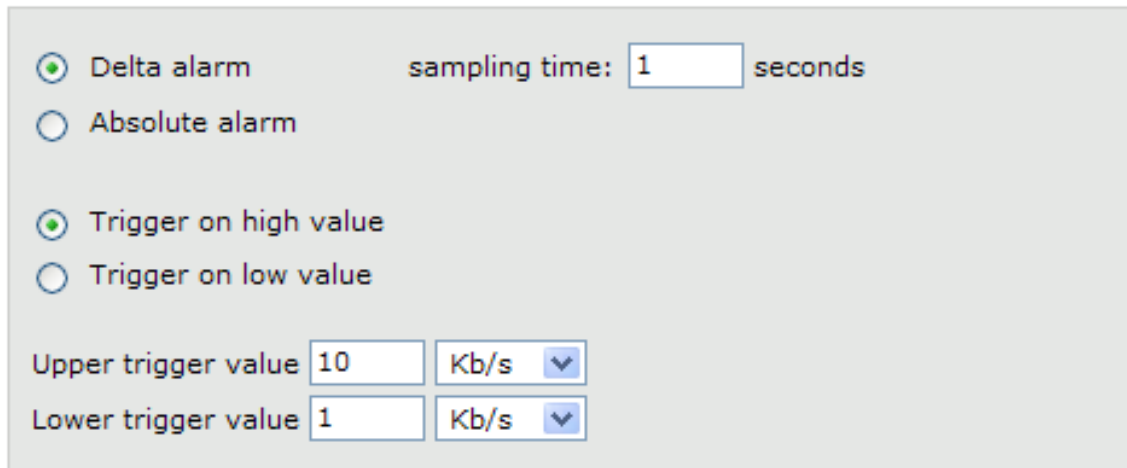
Choose whether you want the alarm to be an absolute or delta alarm. If you choose delta alarm you will also need to enter a sampling time.

Alarms with trigger type upper will trigger when the entries value for the given field increases above the specified upper trigger value. Delta alarms can be triggered multiple times using both trigger values. When the delta value for the alarms entry is lower than the lower trigger value the alarm is reset and can be triggered again.

Only delta alarms can have their trigger type set to lower. A delta alarm with trigger type lower set will be triggered if the delta value for the alarms entry is lower than the lower trigger value. If a upper trigger value is set also, the alarm can be triggered multiple times.

The below image shows setting a delta alarm with sampling time 1 second. The trigger type is set to up-

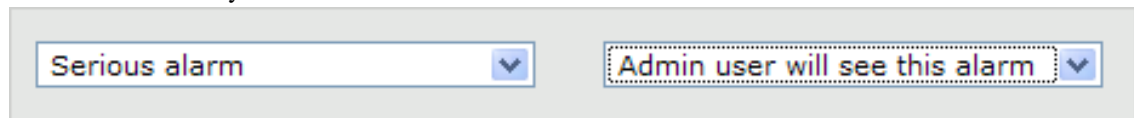
per. The upper trigger value is set to 10 Kb/s and the lower trigger value is set to 1 Kb/s.



The screenshot shows a configuration panel for an alarm. It contains two radio buttons for alarm type: 'Delta alarm' (selected) and 'Absolute alarm'. Next to the 'Delta alarm' radio button is a label 'sampling time:' followed by a text input field containing the number '1' and the word 'seconds'. Below these are two more radio buttons: 'Trigger on high value' (selected) and 'Trigger on low value'. At the bottom, there are two rows of controls. The first row is labeled 'Upper trigger value' and contains a text input field with '10' and a dropdown menu showing 'Kb/s'. The second row is labeled 'Lower trigger value' and contains a text input field with '1' and a dropdown menu showing 'Kb/s'.

Severity and Visibility

The last thing to be done before the alarm can be added is to set the severity and the visibility. Setting the visibility might restrict some types of users from seeing this alarm. The below image show setting a critical alarm which only admin users can see.



The screenshot shows two dropdown menus. The first dropdown menu is labeled 'Serious alarm' and has a downward arrow. The second dropdown menu is labeled 'Admin user will see this alarm' and also has a downward arrow.

Click the "Set alarm" button to add the alarm.

Alarms can be edited in both the "Main" and "Traffic Statistics" tab.

Main

Entry type	Entry	Field	Description	Severity	Type	Trigger type
protocol	1.2048.6.80	Packets		Serious	Absolute	upper
nlhost	10.0.2.26	Packets in		Info	Information	upper
nlmatrix	66.151.234.59 -> 10.0.2.33	Packets		Warning	Warning	upper
alhost	10.0.2.26 - 1.2048.6.139	Bytes in	test	Critical	Critical	upper
almatrix	10.0.2.26 -> 10.0.2.33 - 1.2048.6.139	Bytes		Critical	Absolute	upper

In the "Traffic Statistics" alarms can be edited by choosing "Edit alarm" from the right click menu in the

alarm tables.

Defined alarms						
Entry type	Entry	>>>	<<<	Field	Description	Severity < Type
Protocol	ether.IP.TCP.Http	Packets		Serious Absolute
Host	tpc	Packets in		Critical Absolute
Conversation	www.oasis-open.org -> markuspc	Packets		Information Absolute
Host protocol	tpc - ether.IP.TCP.netbios-ssn	Bytes in		Warning Absolute
Conversation protocol	tpc -> markuspc - ether.IP.TCP.netbios-ssn	Bytes		Serious Absolute
Network card	0:14:22:15:12:9	Packets in		Information Absolute
Network card	0:14:22:15:12:9	Bytes in		Information Absolute
Network card	0:14:22:15:12:9	Bytes in		Information Absolute
Conversation protocol	intranet -> 10.0.2.4 - ether.IP.TCP.Http	Bytes		Information Delta

Add alarm
 Edit alarm
 Delete alarm
 Help

Click to edit the alarm

Network card | 0:14:22:15:12:9 | | | Packets in | | | Information | Absolute | Up

Edit alarm window

Once you have made your changes in the "Edit alarm" window, click "Edit alarm" to change the alarm or click "Clone alarm" to make a copy of the alarm.

Edit alarm

Hosts: 10.0.2.26 Packets in: Packets in

[Enter a description]

☐ Delta alarm sampling time: Seconds
☒ Absolute alarm

☒ Trigger on high value
☐ Trigger on low value

Upper trigger value: 1.0 Packets

Lower trigger value: 0.0

Critical alarm All users will see this alarm

Edit alarm Clone alarm

Edit alarm

Hosts: 10.0.2.26 Packets in: Packets in

[Enter a description]

☐ Delta alarm Sampling time: Seconds
☒ Absolute alarm

☒ Trigger on high value
☐ Trigger on low value

Upper trigger value: 1.0 Packets

Lower trigger value:

Critical alarm All users will see this alarm

Edit alarm Clone alarm

Java Applet Window

Remove alarms

Alarms can be removed from both the "Main" and the "Traffic Statistics" tab. Both triggered and defined alarms can be removed.

Main

In the "Main" tab alarms can be removed by clicking on the delete icon to the right of the alarm in the alarm windows, or by choosing "Delete alarm" in the right click menu.

Defined alarms						
Entry type	Entry	Field	Description	Severity	Type	Trigger type
protocol	1.2048.6.80	Packets		Serious	Absolute	upper
nlhost	10.0.2.26	Packets in		Critical	Absolute	upper
nlmatrix	66.151.234.59 -> 10.0.2.33	Packets		Information	Absolute	upper
alhost	10.0.2.26 - 1.2048.6.139	Bytes in	test		Absolute	upper
almatrix	10.0.2.26 -> 10.0.2.33 - 1.2048.6.139	Bytes			Absolute	upper

Edit alarm
 Delete alarm
 Show triggered alarms
 Help

Click to delete the alarm

Traffic Statistics

In the "Traffic Statistics" tab alarms can be removed by choosing "Delete alarm" from the rightclick

menu.

Defined alarms						
Entry type	Entry	> > >	< Field	Description	Severity	< Type
Protocol	ether.IP.TCP.Http	...	Packets		Serious	Absolute
Host	tpc	...	Packets in		Critical	Absolute
Conversation	www.oasis-open.org -> markuspc	...	Packets		Information	Absolute
Host protocol	tpc - ether.IP.TCP.netbios-ssn	...	Bytes in		Warning	Absolute
Conversation protocol	tpc -> markuspc - ether.IP.TCP.netbios-ssn	...	Bytes		Serious	Absolute
Network card	0:14:22:15:12:9	...	Packets in		Information	Absolute
Network card	0:14:22:15:12:9	...	Bytes in		Information	Absolute
Network card	0:14:22:15:12:9	...	Bytes in		Information	Absolute
Conversation protocol	intranet -> 10.0.2.4 - ether.IP.TCP.Http	...	Bytes		Serious	Delta

Add alarm
Edit alarm
Delete alarm
Help

Click to delete the alarm

Host protocol	tpc - ether.IP.TCP.netbios-ssn	...	Bytes in		Warning	Absolute	Up
---------------	--------------------------------	-----	----------	--	---------	----------	----

Chapter 7. Setup

Overview

The setup screen lets you change settings for the statistics collected, administrate users, setup filter rules as well as configuring the probe. Show the Setup screen by selecting the 'Setup' button on the top of the window. The setup information is shown in windows. Click on a window name in the top menu to a show a setup window.

Collected Statistics	Interval Duration	Interval Time
<input checked="" type="checkbox"/> Protocols	1 hour	10 seconds
<input checked="" type="checkbox"/> Hosts	1 hour	10 seconds
<input checked="" type="checkbox"/> Conversations	1 hour	10 seconds
<input checked="" type="checkbox"/> Protocols per host	1 hour	10 seconds
<input checked="" type="checkbox"/> Protocols per conversation	1 hour	10 seconds
<input checked="" type="checkbox"/> Network cards	1 hour	10 seconds
<input checked="" type="checkbox"/> Network card conversations	1 hour	10 seconds
<input checked="" type="checkbox"/> Network overview	1 hour	5 seconds

Reset settings

Last reset: 26. januar 2007 06:00
Next reset: 26. januar 2007 12:00
Reset day: Every day
Reset hour: Midnight
Reset interval: Every 6 hours

Collected statistics

Statistics Users Filters Probe configuration

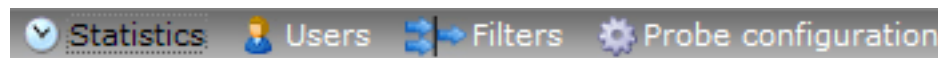
This displays the type of network statistics being collected. You can change the type of statistics collected by setting the checkbox beside each statistics entry and clicking update. If you have a large network

with lots of traffic and problems with the probe using too much memory and processor resources, you can turn off statistics that take much memory.

The interval settings are used for the line chart displaying traffic amount over time. Interval durations can be set from 1 hour to 2 days, and interval times from 10 seconds to 3 hours. A long duration combined with a small time would consume a lot of memory on large networks.

Collected Statistics	Interval Duration	Interval Time
<input type="checkbox"/> Set all	Select a value ▼	Select a value ▼
<input checked="" type="checkbox"/> Protocols	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Hosts	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Conversations	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Protocols per host	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Protocols per conversation	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Network cards	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Network card conversations	1 hour ▼	10 seconds ▼
<input checked="" type="checkbox"/> Network overview	1 hour ▼	5 seconds ▼

Reset interval



This displays the times the network traffic statistics are reset. By default the probe is reset every day starting from midnight and every sixth hour. None of the statistics entries are removed when the probe is reset, but their counters values are set to 0. Entries with no traffic since the last reset will be removed. When reset, the statistics data is saved. Select the 'Data Log' button in the main window to inspect these data.

Reset settings	
Last reset:	29. januar 2007 06:00
Next reset:	29. januar 2007 12:00
Reset day:	Every day ▼
Reset hour:	Midnight ▼
Reset interval:	Every 6 hours ▼
<input type="button" value="Update"/> <input type="button" value="Reset now"/>	

You can configure the day and time when the probe is reset and the time between each reset.

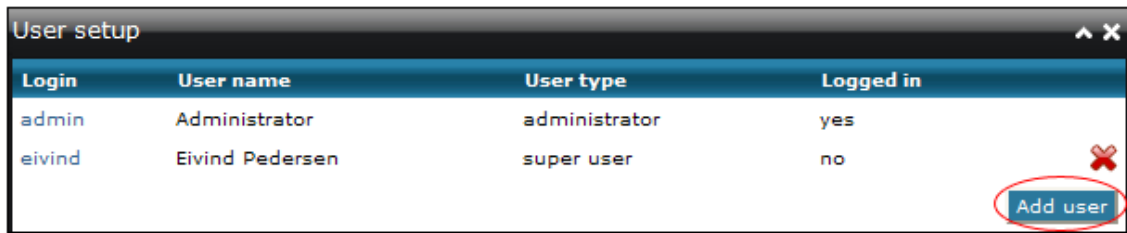
Network interface

Host name resolving

Users and passwords

52

having restricted access to the network statistics data and probe setup. Only administrators and super users can access the user setup.

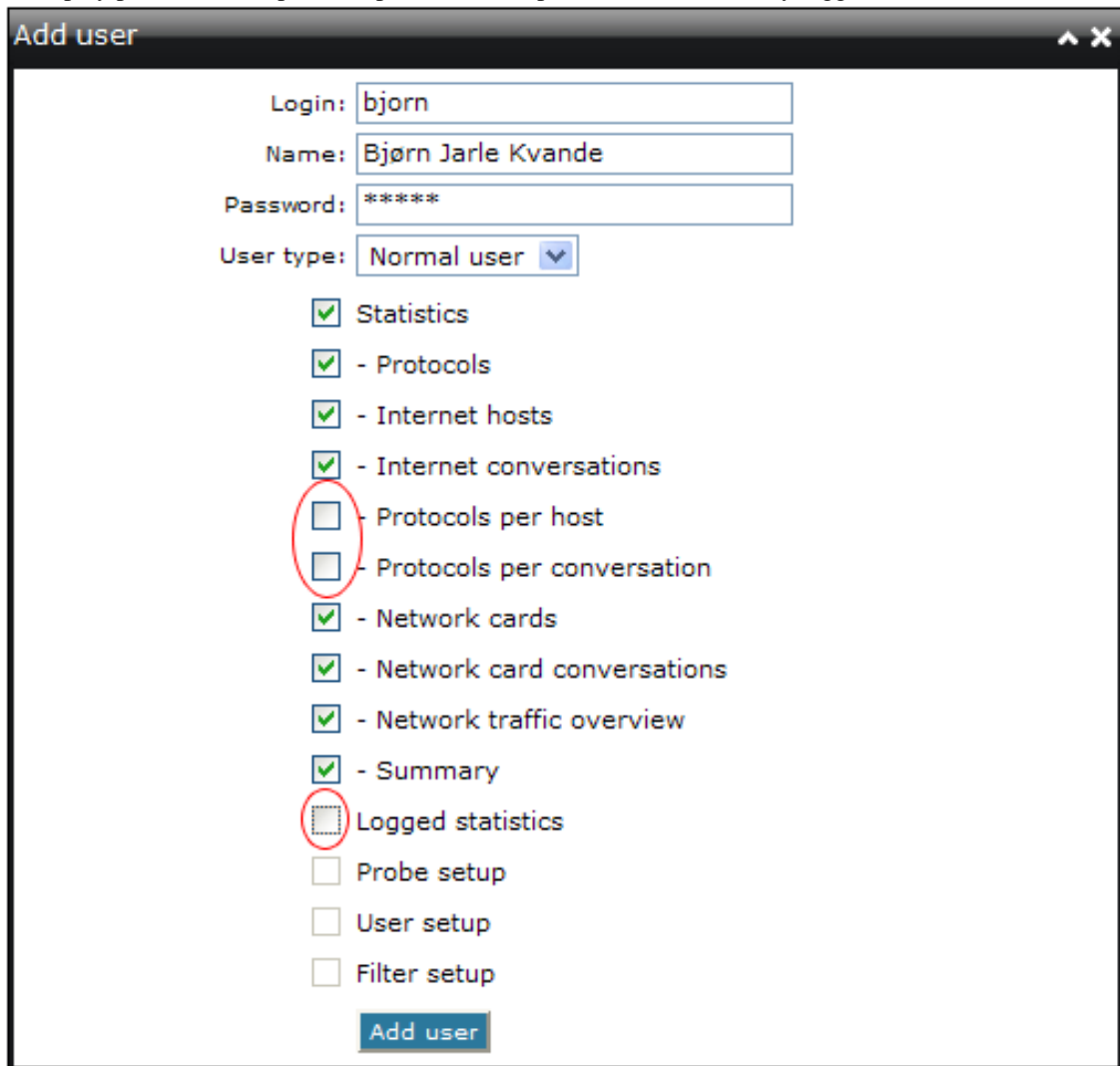


The 'User setup' window displays a table with the following data:

Login	User name	User type	Logged in
admin	Administrator	administrator	yes
eivind	Eivind Pedersen	super user	no

An 'Add user' button is located at the bottom right of the window, circled in red.

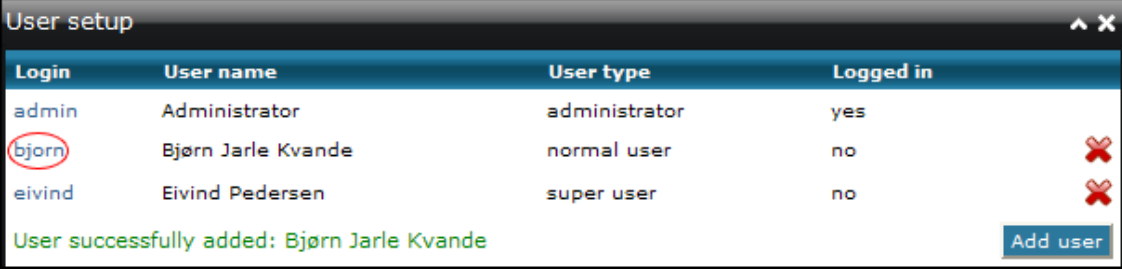
You can add a new user by clicking the 'Add user' button. The below image shows adding the new user 'bjorn' with restricted access to the network statistics data. When this user logs in, he will not have access to display protocols used per host, protocols used per conversation, or any logged statistical data.



The 'Add user' window contains the following fields and options:

- Login:
- Name:
- Password:
- User type: (dropdown menu)
- Statistics: ☒
- Protocols: ☒
- Internet hosts: ☒
- Internet conversations: ☒
- Protocols per host: ☐ (circled in red)
- Protocols per conversation: ☐ (circled in red)
- Network cards: ☒
- Network card conversations: ☒
- Network traffic overview: ☒
- Summary: ☒
- Logged statistics: ☐ (circled in red)
- Probe setup: ☐
- User setup: ☐
- Filter setup: ☐

An 'Add user' button is located at the bottom of the form.



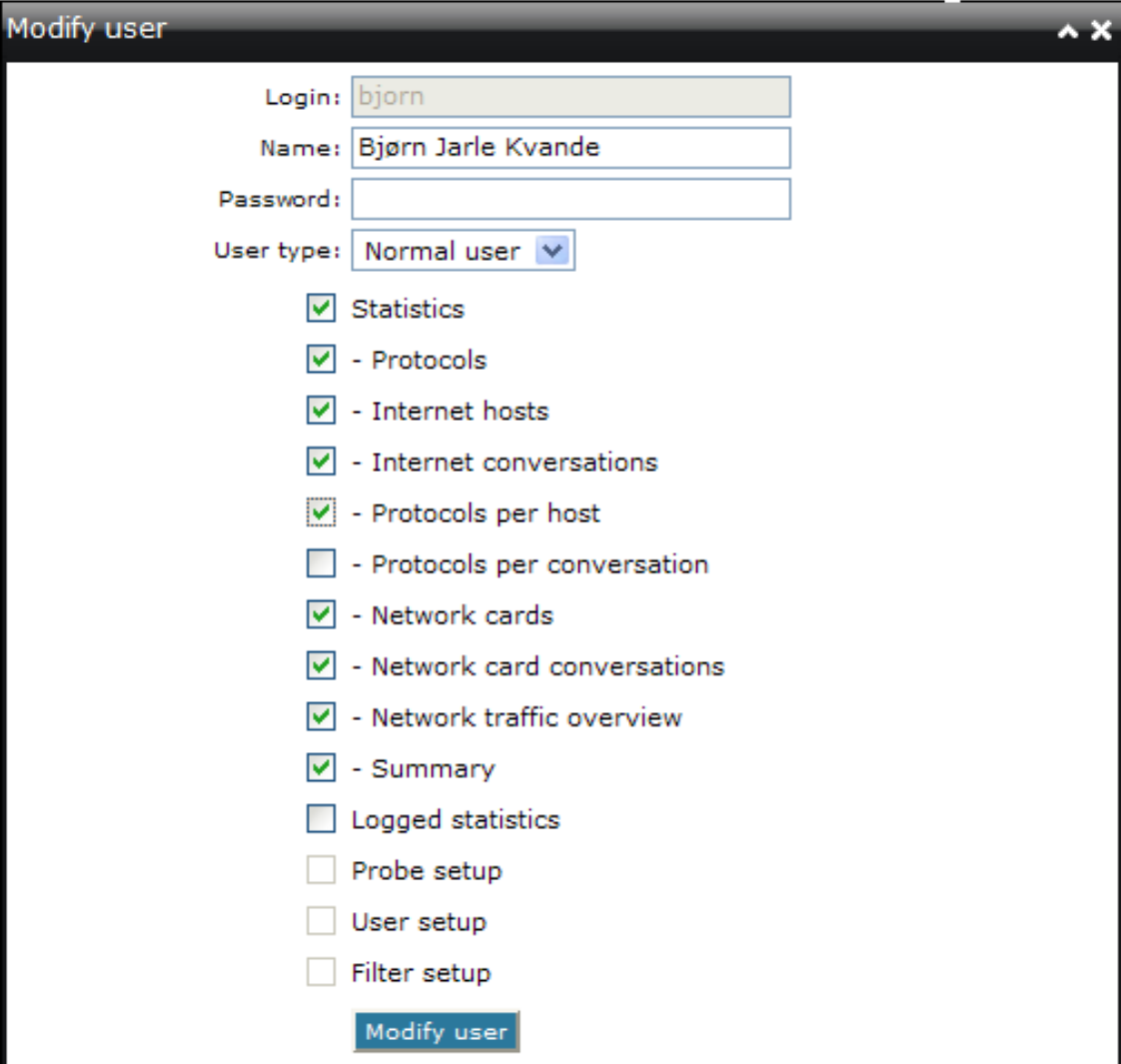
The 'User setup' window displays a table of users. The 'bjorn' user is highlighted with a red circle. Below the table, a green message states 'User successfully added: Bjørn Jarle Kvande'. An 'Add user' button is in the bottom right corner.

Login	User name	User type	Logged in
admin	Administrator	administrator	yes
bjorn	Bjørn Jarle Kvande	normal user	no
eivind	Eivind Pedersen	super user	no

User successfully added: Bjørn Jarle Kvande

Add user

You can modify users by clicking the users login name. The below image modifies the user 'bjorn' and gives him access to display protocols per host. Leave the password field empty to keep the existing password.



The 'Modify user' window shows the configuration for the 'bjorn' user. It includes fields for Login, Name, and Password, and a dropdown for User type. Below these are several checkboxes for permissions, with 'Protocols per host' being the only one that is unchecked. A 'Modify user' button is at the bottom.

Login: bjorn

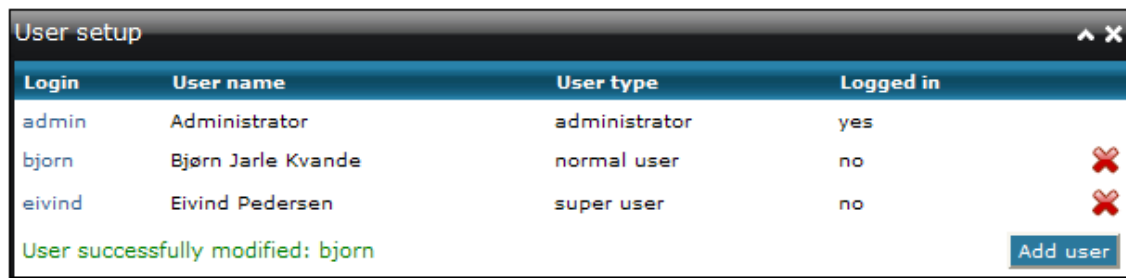
Name: Bjørn Jarle Kvande

Password:

User type: Normal user

- ☒ Statistics
- ☒ - Protocols
- ☒ - Internet hosts
- ☒ - Internet conversations
- ☐ - Protocols per host
- ☐ - Protocols per conversation
- ☒ - Network cards
- ☒ - Network card conversations
- ☒ - Network traffic overview
- ☒ - Summary
- ☐ Logged statistics
- ☐ Probe setup
- ☐ User setup
- ☐ Filter setup

Modify user



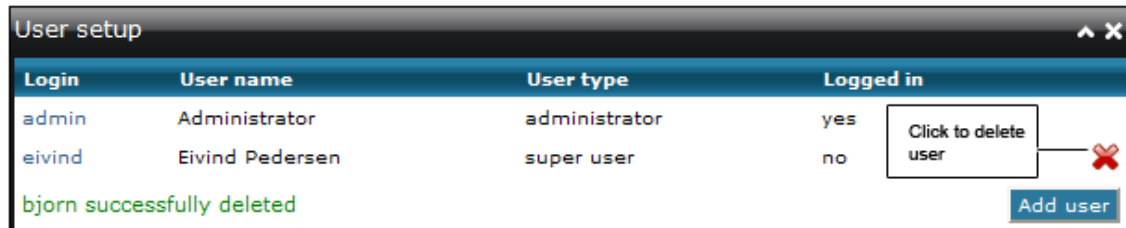
User setup

Login	User name	User type	Logged in
admin	Administrator	administrator	yes
bjorn	Bjørn Jarle Kvande	normal user	no
eivind	Eivind Pedersen	super user	no

User successfully modified: bjorn

Add user

Delete a user by clicking the delete button to the right for the user. In the below image the user bjorn has been deleted.



User setup

Login	User name	User type	Logged in
admin	Administrator	administrator	yes
eivind	Eivind Pedersen	super user	no

bjorn successfully deleted

Add user

Filters

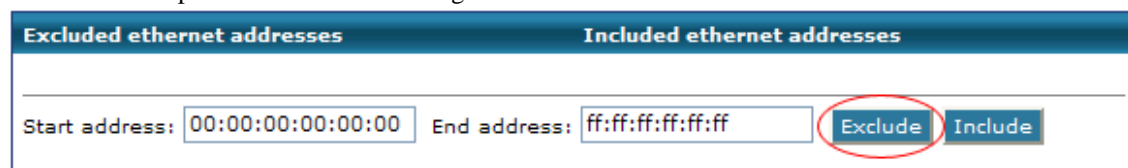


Filtering out some network traffic reduces the memory consumption, and makes it easier to monitor specific hosts or ports. By default there are no filter rules defined, and all traffic will be picked up.

Ethernet address filters

"Excluded" traffic is never picked up by the probe, while "included" traffic is always picked up, overriding any exclusion rule.

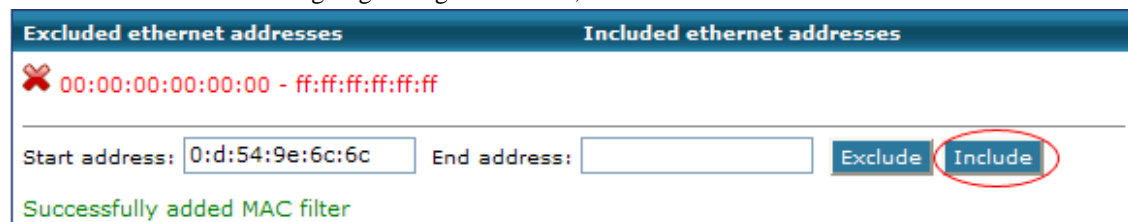
You can filter traffic on specific network cards or ranges of network cards, by adding the ethernet (MAC) address. For a single network card, add the ethernet address in one of the fields. For a range, add the start and stop address. The below image shows how to exclude all traffic.



Excluded ethernet addresses Included ethernet addresses

Start address: 00:00:00:00:00:00 End address: ff:ff:ff:ff:ff:ff **Exclude** Include

We want to include address going through our router, which has the address 0:d:54:9e:6c:6c



Excluded ethernet addresses Included ethernet addresses

✗ 00:00:00:00:00:00 - ff:ff:ff:ff:ff:ff

Start address: 0:d:54:9e:6c:6c End address: **Exclude** **Include**

Successfully added MAC filter

Excluded ethernet addresses	Included ethernet addresses
✖ 00:00:00:00:00:00 - ff:ff:ff:ff:ff:ff	✖ 00:0d:54:9e:6c:6c
Start address: 0:d:54:9e:6c:6c End address: <input type="text"/>	Exclude Include
Successfully added MAC filter	

To delete a rule, simply click the red delete icon.

IP address filters

You can add a new IP filter rule by defining the start IP and end IP (a range). If it's only a single IP address, let start and end have the same value. Valid IP addresses are from 0.0.0.0 - 255.255.255.255. The below image shows adding the new IP exclusion rule, 10.0.1.1 - 10.0.1.255.

Excluded IP addresses	Included IP addresses
Start address: 10.0.1.1 End address: 10.0.1.255	Exclude Include

But we want to pick up all traffic generated by the IP address 10.0.1.25:

Excluded IP addresses	Included IP addresses
✖ 10.0.1.1 - 10.0.1.255	
Start address: 10.0.1.25 End address: 10.0.1.25	Exclude Include
Successfully added IP filter	

These are the filter rules defined so far:

Excluded IP addresses	Included IP addresses
✖ 10.0.1.1 - 10.0.1.255	✖ 10.0.1.25
Start address: 10.0.1.25 End address: 10.0.1.25	Exclude Include
Successfully added IP filter	

To delete a rule, simply click the red delete icon.

Protocol filters

Filter rules for protocols/port numbers can be set the same way: Choose the protocol type (TCP, UDP, IP or Ethernet), the port number range and click the 'Include' or 'Exclude' button. The example below shows that all TCP traffic going on port 1 - 200 is never picked up by the probe, except TCP traffic on port 80 (HTTP) and port 22 (SSH).

Excluded ports	Included ports
✖ tcp port 1 - 200	✖ tcp port 80 ✖ tcp port 22
TCP Start port: 22 End port: <input type="text"/>	Exclude Include
Successfully added protocol filter	

Chapter 8. Advanced

Manually starting the probe

Open a command line window or console, and cd to the directory where Network Probe is installed.

MS Windows with Sun Java VM: NOTE: You should always add at least "-Xmx256m" as the first parameter to the java command, otherwise the probe would run out of memory quite soon.

```
C:\Program Files\Network Probe 2>java -Xmx256m -jar Probe.jar
Probe startup initialized...
loading protocol definitions...
Adapter MELCO WLI-PCM-L11 Wireless LAN Adapter successfully opened
Probe is running
Please open http://windows:7030/ in your web browser
```

Linux with Sun Java VM: NOTE: You should always add at least "-Xmx256m" as the first parameter to the java command, otherwise the probe would run out of memory quite soon.

```
$java -Xmx256m -jar Probe.jar
Probe startup initialized...
loading protocol definitions...
These are the network adapters installed on your computer:
ID, Adapter name
 1, en0
 2, en1

Please enter the ID for the adapter you wish to use or enter 0 to quit: 2
You chose en1
Probe is running
Please open http://linux:7030/ in your web browser
```

Starting the stand-alone client

Open a command line window or console, and cd to the directory where Network Probe is installed. Remember to start the probe first.

```
C:\Program Files\Network Probe 2>java -jar wwwroot/Client.jar
```

Command line options

- **-port 7031** - this will set the probe login port to 7031, the default port is 7030.
- **-card 1** - if you have multiple network interfaces this will select network card number 1.
- **-r frames.dat 1000** - this will record 1000 network packets to the file frames.dat and then stop
- **-p frames.dat** - will read network packets from the frames.dat file and stop
- **-home "C:\Program Files\Network Probe 2"** - sets the probe home directory if you start it from an-

other directory

- **-nostart** - starts the probe, but not the packet decoding. This is useful if you have a large network with lots of traffic and need to configure the probe to avoid excess memory usage and CPU load.
- **-noprom** - starts the probe in non-promiscuous mode, meaning that only traffic to/from the probing computer will be picked up. All broadcast traffic is picked up as well.
- **-silent** - the probe will run in silent mode and not send out DNS requests to resolve IP addresses to host names.
- **-nointerval** - starts the probe without interval statistics being collected.
- **-noip** - starts the probe with a NIC not assigned with an IP
- **-dump** - this will dump the packet content to the console. [Click here for details.](#)
- **-stats host,matrix,nlhost,nlmatrix,alhost,almatrix,protocol,network** - starts the probe with a limited set of packet decoding
 - host** - collect statistics about network cards (low memory usage)
 - matrix** - collect statistics about network card conversations (low memory usage)
 - nlhost** - collect statistics about hosts (medium memory usage)
 - nlmatrix** - collect statistics about conversations (medium memory usage)
 - alhost** - collect statistics about protocols per host (high memory usage)
 - almatrix** - collect statistics about protocols per conversation (high memory usage)
 - protocol** - collect statistics about protocols (low memory usage)
 - network** - collect statistics about the network (low memory usage)
- **-loadtest** - prints out network load statistics. The test takes one minute, and the output can tell if the network is heavily loaded or not - and how diversified the traffic is.
- **-systray** - start the windows systray icon.
- **-showlog** - open the probe log window.
- **-client** - start the client after probe startup.
- **-resetpassword** - resets the password for the admin user.
- **-verbose** - a debug mode. More detailed error messages are shown if the probe has problems.
- **-import "C:\Program Files\Network Probe1.3\statistics"** - imports data from 1.x versions of the probe. This will import data from the probe installation in "C:\Program Files\Network Probe 1.3".

Resetting the admin password

In case you forget the administrator password, start Network Probe "manually" from command line with the "-resetpassword" parameter:

```
java -jar Probe.jar -resetpassword
```

Dump packet content to the console

Using the command line option `-dump` you can print the content of selected packets to the console.

The following will dump all the packets seen by the probe

```
java -jar Probe.jar -dump
```

```
....
Ethernet - 00:02:2d:0c:1f:80 -> 00:04:e2:60:66:a2
Ethernet - payload: 800
          IP - 10.0.1.20 -> 158.39.26.220
          IP - length: 87
          IP - payload: 17
          UDP - 2002 -> 53
          DNS - operation: DNS query
000: 03 31 30 30 01 31 01 30 02 31 30 07 69 6e 2d 61 .100.1.0.10.in-a
016: 64 64 72 04 61 72 70 61 00 00 0c 00 01 00 00 00 ddr.arp.....
032: 00
          Ethernet - 00:04:e2:60:66:a2 -> 00:02:2d:0c:1f:80
          Ethernet - payload: 800
          IP - 158.39.26.220 -> 10.0.1.20
          IP - length: 164
          IP - payload: 17
          UDP - 53 -> 2002
          DNS - operation: DNS response
000: 03 31 30 30 01 31 01 30 02 31 30 07 69 6e 2d 61 .100.1.0.10.in-a
016: 64 64 72 04 61 72 70 61 00 00 0c 00 01 c0 14 00 ddr.arp.....?..
032: 06 00 01 00 00 1c 05 00 41 08 70 72 69 73 6f 6e .....A.prison
048: 65 72 04 69 61 6e 61 03 6f 72 67 00 0a 68 6f 73 er.iana.org..hos
064: 74 6d 61 73 74 65 72 0c 72 6f 6f 74 2d 73 65 72 tmaster.root-ser
080: 76 65 72 73 c0 43 77 54 00 00 00 00 00 00 00 00 vers?CwT.....
096: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

The first lines display the protocols of the packet, Ethernet, IP, and UDP. The first packet above is a DNS query to the name server (port 53 on top of UDP and IP). The second packet seen is the reply from the name server with the answer to the query.

This will dump all the packets transmitted or received by the host with IP 10.0.1.20:

```
java -jar Probe.jar -dump 10.0.1.20
```

This will dump all the HTTP packets seen by the probe:

```
java -jar Probe.jar -dump :1.2048.6.80
```

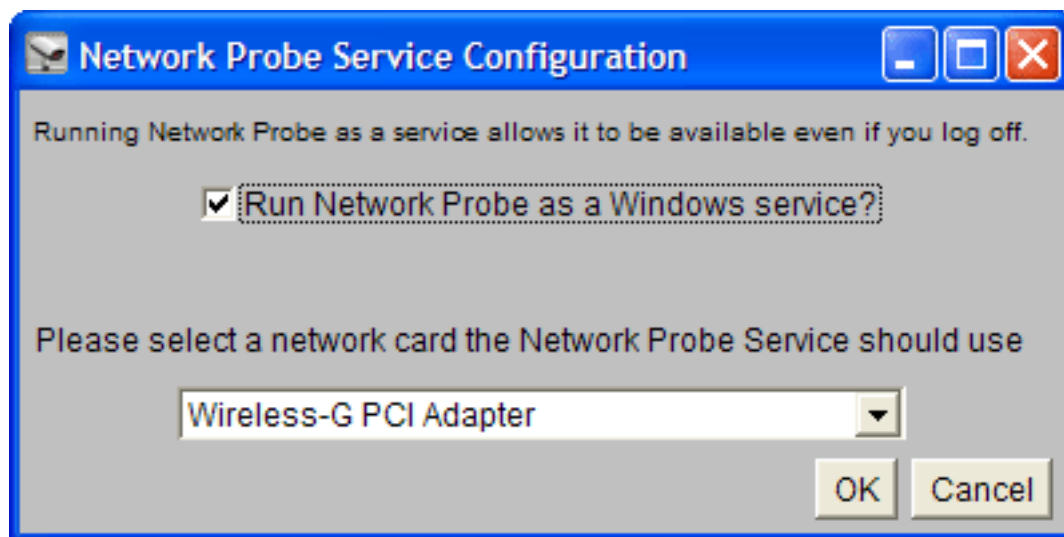
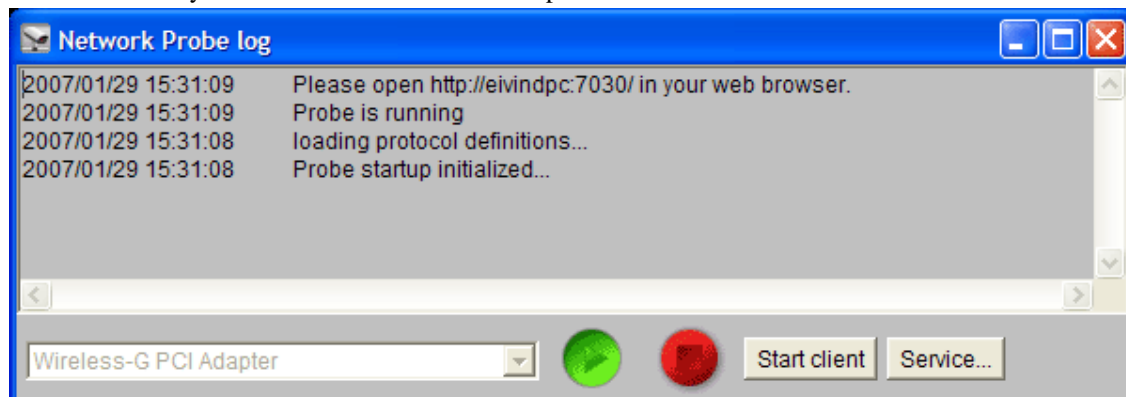
1 is for ethernet, 2048 is IP (0x800), 6 is for TCP, and 80 is the HTTP port number.

This will dump all the HTTP traffic for the host with IP 10.0.1.20:

```
java -jar Probe.jar -dump 10.0.1.20:1.2048.6.80
```

Running the probe as a Windows service

Running it as a Windows service allows it to stay in background even if no users are logged in, and it will automatically be launched on Windows startup.



Automatically starting the probe on *NIX

The "netprobe" script makes the probe stay in background. To automate this on startup, add the following to your startup procedure script:

```
cd /path-to-netprobe
./netprobe start
```

On Red Hat Linux, you can put it in the file `/etc/rc.local`. The logged messages are stored in `/var/log/networkprobe.log`

Configure web browsers to use Java (Linux)

For Mozilla (remember to enable java in the browser):

- 1) cd to `/usr/lib/mozilla/plugins` (or where Mozilla is installed)
- 2) create the following symbolic link:

```
ln -s /usr/java/j2sdk1.4.2_01/plugin/i386/ns610/libjavaplugin_oji.so libjavaplugin_oji.so
(replace with path to your Java installation)
```

For Netscape (remember to enable java in the browser):

- 1) cd to `/usr/local/netscape/plugins` (or where Netscape is installed)
- 2) create the following symbolic link:

```
ln -s /usr/java/j2sdk1.4.2_01/plugin/i386/ns610-gcc32/libjavaplugin_oji.so libjavaplugin_oji.so
(replace with path to your Java installation)
```

For Opera:

- 1) Select Edit->Preferences->Multimedia->Java path
- 2) Set it to `/usr/java/j2sdk1.4.2_01/jre/lib/i386` (replace with path to your Java installation)

Starting the probe with no IP assigned to the interface

The probe must be started manually with the `"-noip"` parameter if the NIC doesn't have an IP assigned to it:

```
java -jar Probe.jar -noip
Probe startup initialized...
loading protocol definitions...
Enter name of network device to open (i.e. eth0): eth1
Probe is running
Please open http://linux:7030/ in your web browser.
```

On *NIX, you can use the device name as parameter to `"-noip"`, to avoid interaction:

```
java -jar Probe.jar -noip eth0
Probe startup initialized...
loading protocol definitions...
Probe is running
Please open http://linux:7030/ in your web browser.
```

Performance tuning

Network Probe installed on a network having a lot of diversified traffic (many hosts with many conversations), will consume a lot of memory if not reset frequent enough. By default it is reset every 6th hour, but this can be adjusted down to every hour. The following might solve memory problems as well:

1. Turn off interval data, reduce interval duration and/or increase interval time
2. Use filters to include only certain type of traffic
3. Start Network Probe from command line with larger maximum Java heap size (defaults to 256 MB):

```
C:\Program Files\Network Probe 2\java -Xmx512m -jar Probe.jar
```

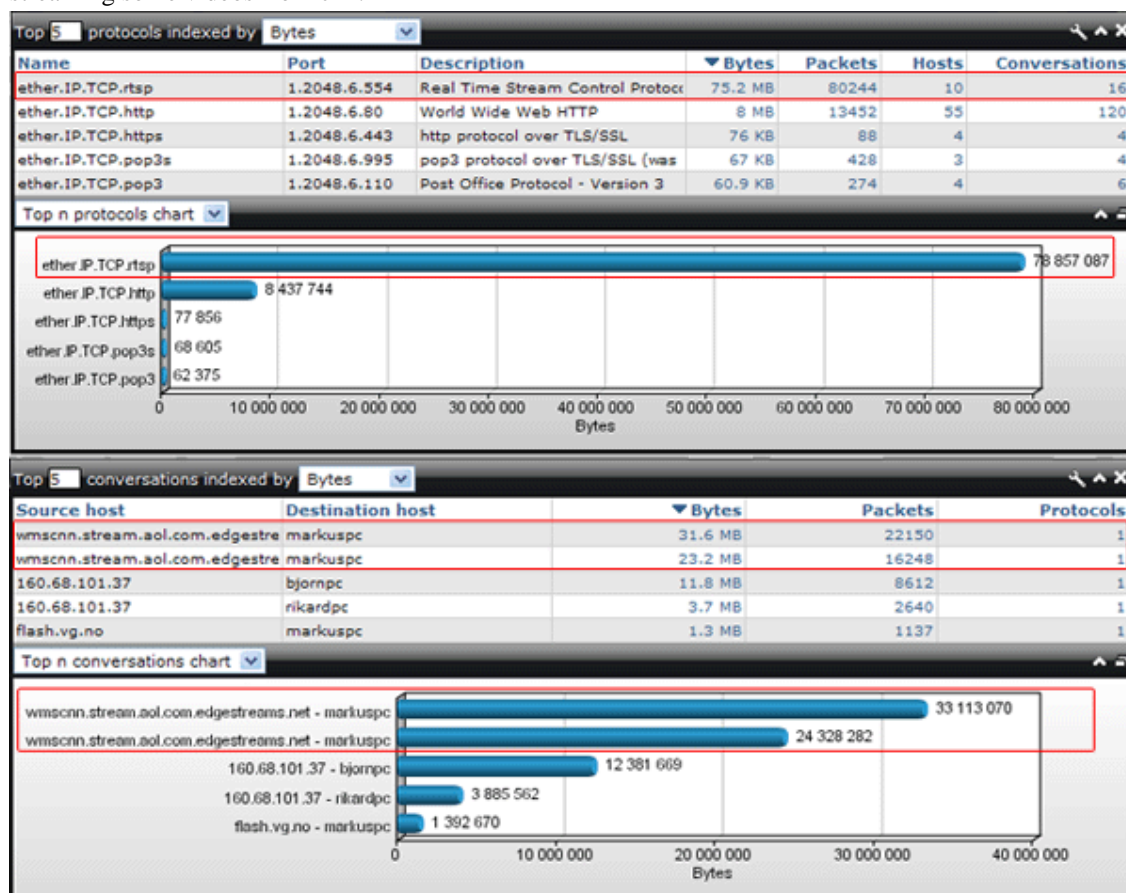
Heavy CPU usage is normally caused by the chart generation process, when there are many intervals.

Chapter 9. Practical Use

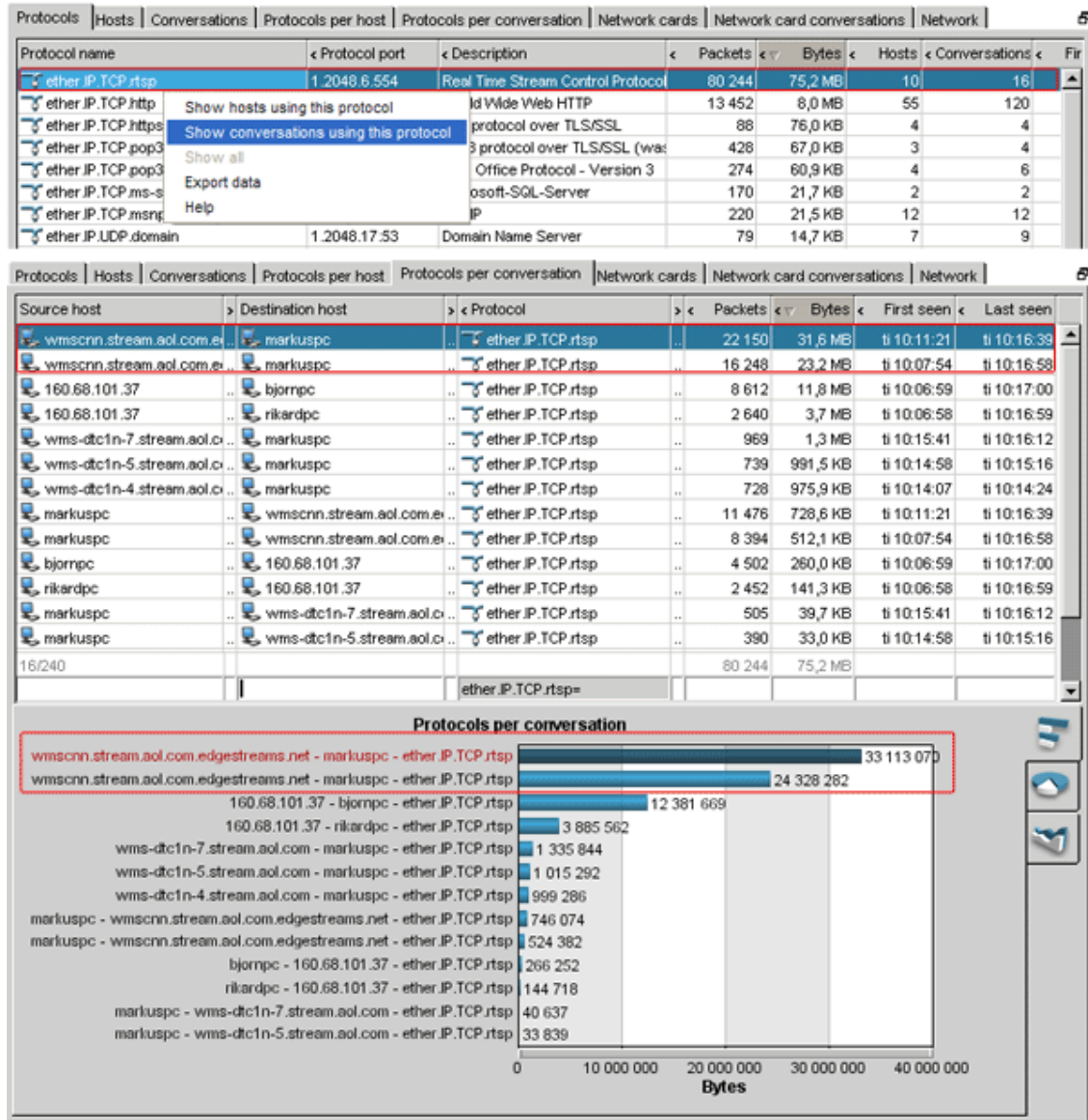
Slow network

If your network is crawling to a standstill, and you suspect there might be a problem with the network traffic, Network Probe will quickly help you identify what is causing the problem and show you who is generating any troublesome traffic. The first thing you see when you log on to Network Probe is the Main screen. The Main screen gives you an instant overview over the top protocols, hosts and conversations. Using the Main screen you can quickly identify the protocol and host using up your bandwidth.

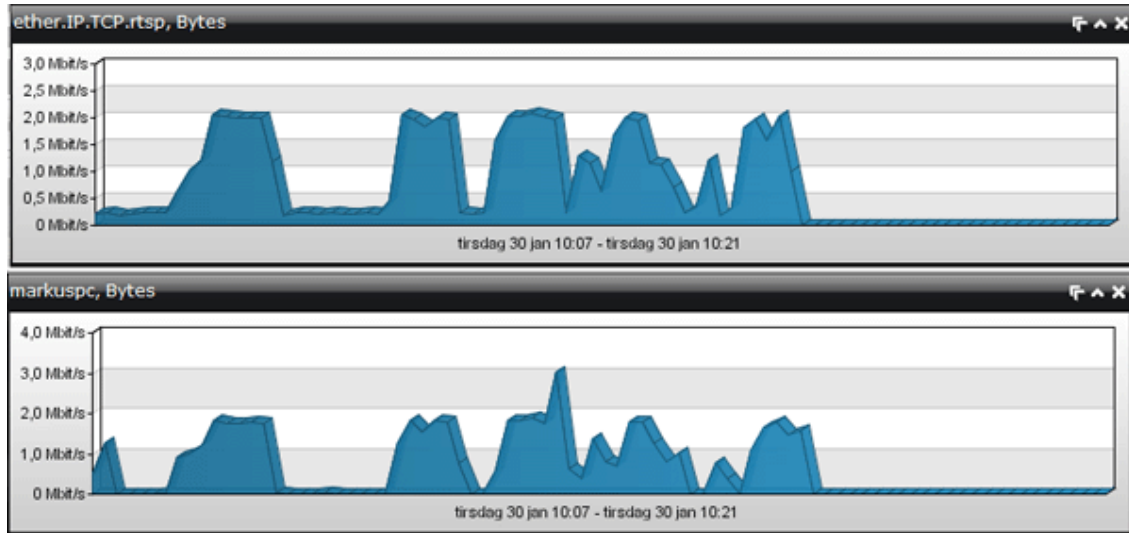
In the top protocols window you can see that rtsp is using a substantial part of the bandwidth. In the top host window you can see that markuspc is using the most bandwidth, and in the top conversations window you see that markuspc has two conversations with streams from cnn. Markuspc is most likely streaming some videos from cnn.



To get more details you can use the applet in the Traffic Statistics screen. In the "Protocols" tab right click on ether.IP.TCP.rtsp and click on "Show conversations using this protocol". This will open the "Protocols per conversation" tab. As in the top conversations window you see that markuspc has two conversations with streams from cnn. The first stream started 10:07 and the second at 10:11. Both streams were last seen at 10:16.

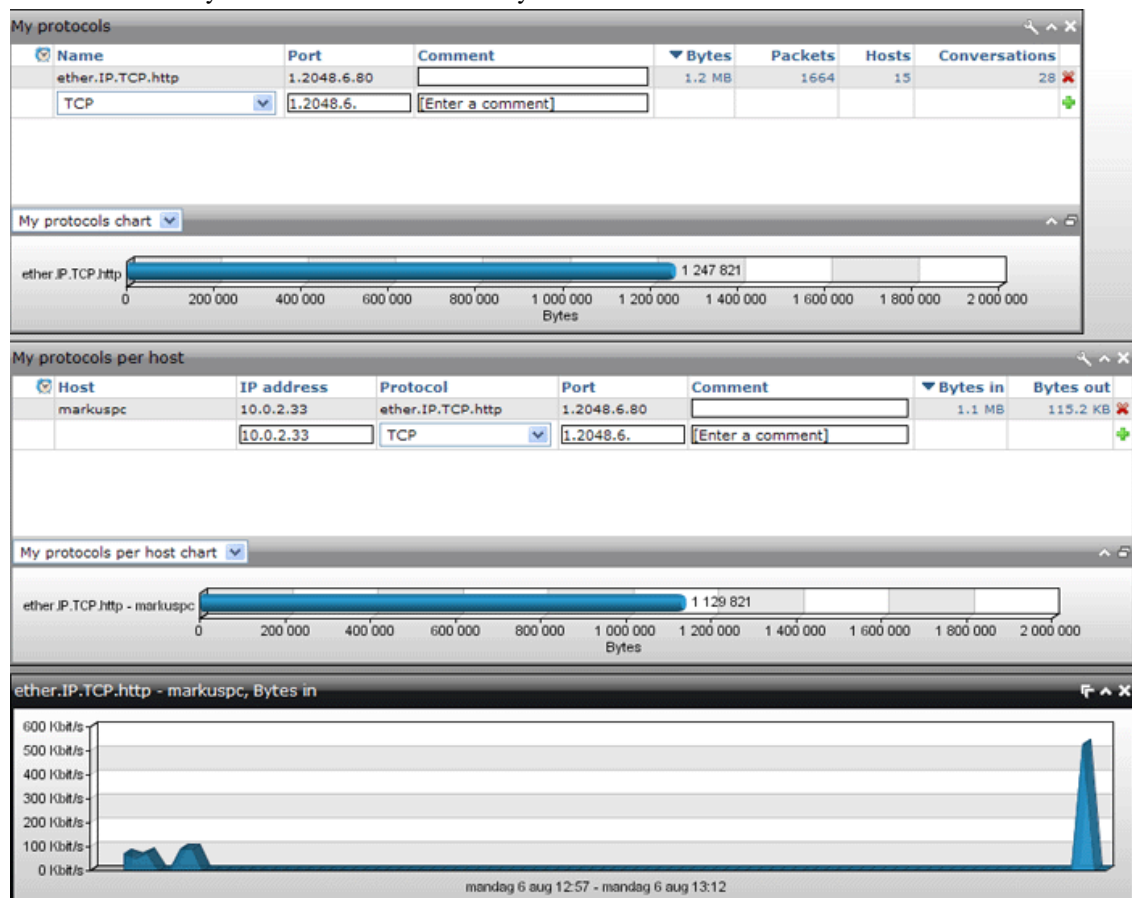


Now that you have identified the source of your network slowdown, you can use Network Probe to check if the host markuspc actually stops watching videos on cnn. To do this you can detach the interval chart for rtp in the top protocols window, and the interval chart for markuspc in the top hosts window. You can also do this by detaching the interval chart for the two streams in the top conversations window.

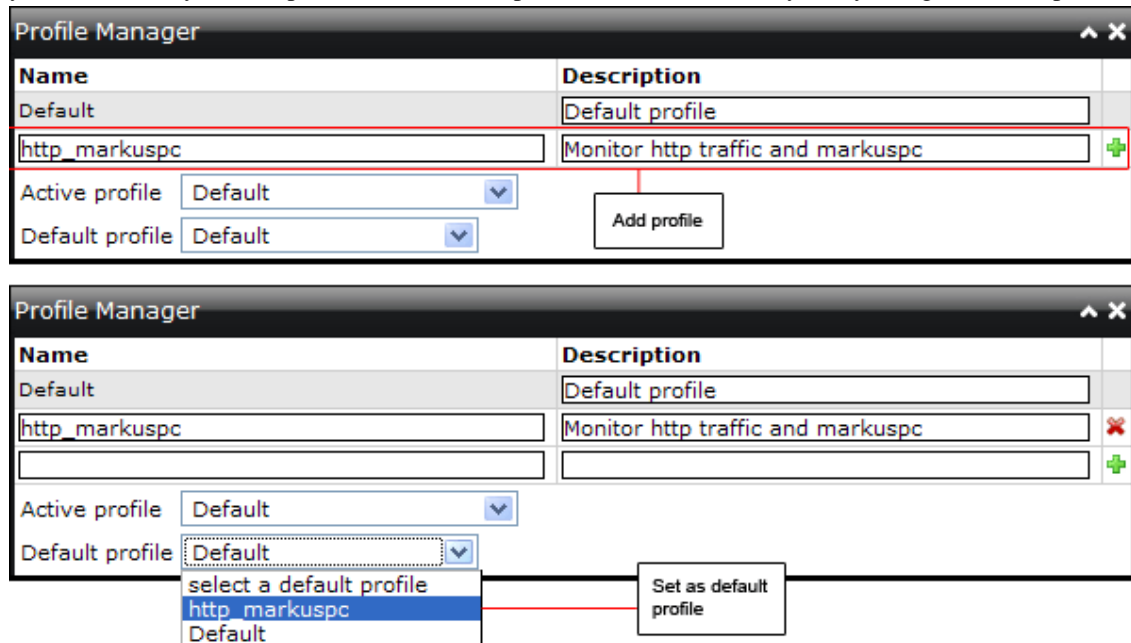


Monitoring

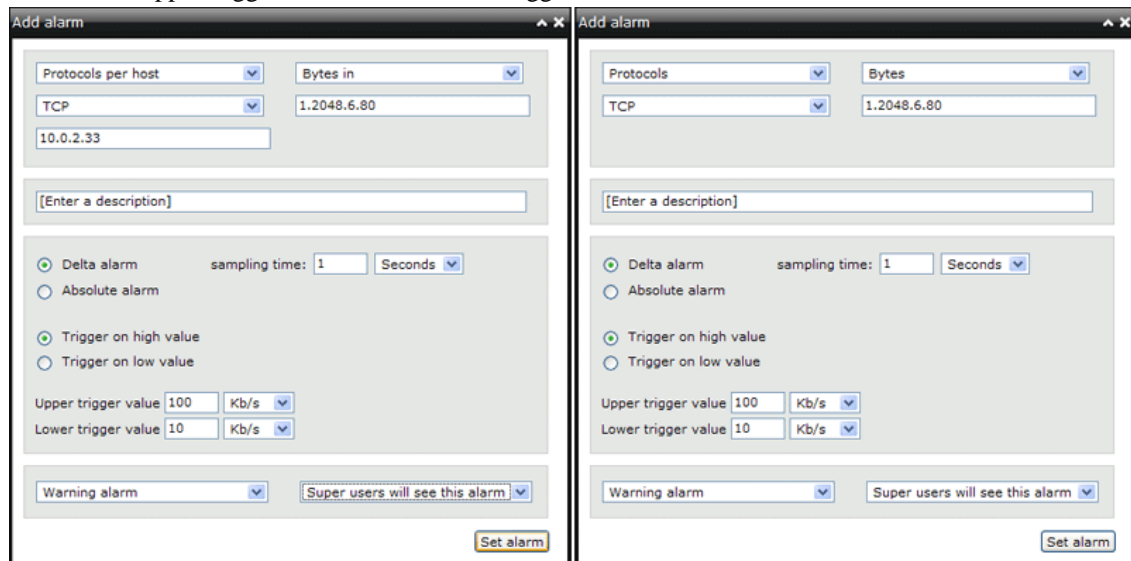
Network Probe lets you easily monitor different hosts, conversations or protocols on your network. Say you want to monitor how much hosts on your network surf on the internet, especially you want to monitor http traffic to host markuspc. To monitor the http traffic on you network open the "My protocols" window and enter 1.2048.6.80. Http traffic to host markuspc can be monitored using the "My protocols per host" window. Open the "My protocols per host" window and enter markuspc and 1.2048.6.80, also you could detach the byte interval chart for this entry.



Now create a new profile, name it for example markus_http. The profile saves the layout of the Main screen. Later on you can easily activate the profile and monitor the http protocol and host markuspc. If you set the newly created profile as the default profile it is activated everytime you log on the the probe.



If you do not want to manually watch the traffic you can set some alarms to let Network Probe watch the entries for you. Add an alarm for the http protocol and one for markuspc using the http protocol. To monitor the total amount of bandwidth used by the entries use an absolute alarm, to monitor how much the entry increases in given time intervals use a delta alarm. The below image shows adding two alarms, one for the http protocol and one for markuspc using the http protocol. Both alarms are set to be delta alarms with upper trigger 100 Kb/s and lower trigger value 10 Kb/s.



Defined and triggered alarms can later on be viewed in the "Defined alarms" and "Triggered alarms" window.

Defined alarms							
Entry type	Entry	Field	Description	Severity	Type	Trigger type	
protocol	1.2048.6.80	Bytes		Warning	Delta	upper	✖ ✓
alhost	10.0.2.33 - 1.2048.6.80	Bytes in		Warning	Delta	upper	✖ ✓

Triggered alarms							
Time ▼	Count	Entry type	Entry	Field	Description	Value	Severity
6. august 2007 15:15:58	5	alhost	10.0.2.33 - 1.2048.6.80	Bytes in		205.3 Kbit/s	Warning
6. august 2007 15:15:58	5	protocol	1.2048.6.80	Bytes		243.6 Kbit/s	Warning