# **Network Probe User Guide**

Network Probe User Guide		

http://www.objectplanet.com/probe

#### **Table of Contents**

2. Installation       2         Windows installation       3         Mae installation       4         License key       5         Deployment       5         System requirements       7         3. Main       9         Overview       9         Windows       9         Top n windows       11         Summary window       12         My Windows       13         13 Profiles       15         Profiles       15         Profiles       15         Profile Manager       15         Switch profiles       15         4. Traffic Statistics       17         Overview       17         Applet interface overview       17         Switching network traffic view       18         Detaching a tab to a window       19         Collapsing and resizing a table column       20         Collapsing and resizing a table column       20         Scarching for network traffic details       22         Filtering network traffic data       24         Exporting network traffic data       24         Exporting network traffic data       24         Exporting network t	1. Introduction	
Linux installation       3         Mae installation       4         License key       5         Deployment       5         System requirements       7         3. Main       9         Overview       9         Windows       9         To pusindows       11         Summary window       12         My Windows       13         Alarm windows       13         Profiles       15         Profiles       15         Profile Manager       15         Switch profiles       15         4. Traffic Statistics       17         Overview       17         Applet interface overview       17         Switching network traffic view       18         Detaching a tab to a window       19         Collapsing and resizing a table column       20         Collapsing and resizing a table column       20         Colapsing the data in the charts       20         Sorting a table column       20         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network		
Mac installation     4       License key     5       Deployment     5       System requirements     7       3. Main     9       Overview     9       Windows     9       Top n windows     11       Summary window     12       My Windows     13       Alarm windows     13       Profiles     15       Profiles     15       Profiles     15       Switch profiles     15       4. Traffic Statistics     17       Overview     17       Applet interface overview     17       Switching network traffic view     18       Detaching a tab to a window     19       Collapsing and resizing a table column     20       Changing the data in the charts     20       Sorting a table column     22       Searching for network traffic details     22       Filtering network traffic details     22       Filtering network traffic details     23       Viewing more detail     24       Exporting network traffic details     23       Frotocols per conversation     30       Network cards     34       Network cards     34       Network cards     38       Alarms<		
License key         5           Deployment         5           System requirements         7           3. Main         9           Overview         9           Windows         9           Top in windows         12           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Collapsing and resizing a table column         20           Collapsing and resizing a table column         22           Searching for network traffic details         22           Filtering network traffic details         22           Filtering network traffic details         22           Fortococls         25           Hosts         25           Conversations         28		
Deployment         5           System requirements         .7           3. Main         .9           Overview         .9           Windows         .9           Top n windows         .11           Summary window         .12           My Windows         .13           Alarm windows         .13           Alarm windows         .13           Profiles         .15           Profiles         .15           Profile Manager         .15           Switch profiles         .15           4. Traffic Statistics         .17           Overview         .17           Applet interface overview         .17           Switching network traffic view         .18           Detaching a tab to a window         .19           Collapsing and resizing a table column         .20           Collapsing and resizing a table column         .20           Contagning the data in the charts         .20           Sorting a table column         .22           Searching for network traffic details         .22           Searching for network traffic details         .22           Silvering more detail         .24           Exporting network traffi	Mac installation	4
System requirements         7           3. Main         9           Overview         9           Windows         9           Top n windows         11           Summary window         12           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         22           Viewing more detail         22           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         32           Net	License key	5
3 Main         9           Overview         9           Windows         9           Top n windows         11           Summary window         12           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4 Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching at ab to a window         19           Collapsing and resizing a table column         20           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Searching for network traffic details         22           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         25 <tr< td=""><td>Deployment</td><td>5</td></tr<>	Deployment	5
Overview         9           Windows         11           Top n windows         11           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4 Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Collapsing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         38           Network cards         34	System requirements	7
Windows         11           Summary window         12           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Eiltering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         38           Network cards         34           Network cards         34           Network cards         38	3. Main	9
Top n windows         11           Summary window         12           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Colapsing and resizing a table column         20           Searching for network traffic details         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         25           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network cards         34           Network cards	Overview	9
Summary window         12           My Windows         13           Alarm windows         13           Profiles         15           Profiles         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Viewing more detail         24           Exporting network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         25           Conversations         28           Protocols per host         30           Rotwork cards         34           Network card conversations         36           Network card conversations	Windows	9
My Windows     13       Alarm windows     13       Profiles     15       Profiles     15       Profile Manager     15       Switch profiles     15       4. Traffic Statistics     17       Overview     17       Applet interface overview     17       Switching network traffic view     18       Detaching a tab to a window     19       Collapsing and resizing a table column     20       Collapsing and resizing a table column     20       Sorting a table column     22       Searching for network traffic details     22       Filtering network traffic details     23       Viewing more detail     24       Exporting network traffic data     24       Protocols     25       Hosts     25       Conversations     28       Protocols per host     30       Protocols per host     30       Protocols per conversation     32       Network cards     34       Network card conversations     36       Network card conversations     36       Network card conversations     36       Network dards     34       Alarms     43       Jospilay logged statisitics     43       Log manager	Top n windows	11
Alarm windows       13         Profiles       15         Profiles       15         Profile Manager       15         Switch profiles       15         4. Traffic Statistics       17         Overview       17         Applet interface overview       17         Switching network traffic view       18         Detaching a tab to a window       19         Collapsing and resizing a table column       20         Sorting a table column       20         Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       33         Alarms       39         Alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview	Summary window	12
Profiles         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network cards         34           Network card conversations         36           Network         38           Alarms         39           Defined alarms         40           Alarms         43           Logged interval data         4		
Profile Nanager         15           Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         18           Detaching a tab to a window         18           Collapsing and resizing a table column         20           Cohanging the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network cards         34           Network cards         34           Network card conversations         36           Network large can be conversations         36           Network card conversations         36           Network large can be conversations         36           Network large can be conversations	Alarm windows	13
Profile Manager         15           Switch profiles         15           4. Traffic Statistics         17           Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Conting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         25           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network card         34           Network card conversations         36           Network         38           Alarms         39           Defined alarms         40           Alarms         39           Overview         43           Overview         43           Log and interval data         44 <t< td=""><td>Profiles</td><td> 15</td></t<>	Profiles	15
Switch profiles       15         4. Traffic Statistics       17         Overview       17         Applet interface overview       17         Switching network traffic view       18         Detaching a tab to a window       19         Collapsing and resizing a table column       20         Changing the data in the charts       20         Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Logged interval data       44		
4. Traffic Statistics       17         Overview       17         Applet interface overview       18         Detaching a tab to a window       19         Collapsing and resizing a table column       20         Changing the data in the charts       20         Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarms       43         Log diterval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50	Profile Manager	15
Overview         17           Applet interface overview         17           Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network cards         34           Network card conversations         36           Network         38           Alarms         39           Triggered alarms         39           Defined alarms         40           Alarm action library         41           5. Traffic Log         43           Overview         43           Log and interval data         44           Log and interval data <td>Switch profiles</td> <td> 15</td>	Switch profiles	15
Applet interface overview       17         Switching network traffic view       18         Detaching a tab to a window       19         Collapsing and resizing a table column       20         Changing the data in the charts       20         Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47 <td>4. Traffic Statistics</td> <td> 17</td>	4. Traffic Statistics	17
Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network cards         34           Network card conversations         36           Network         38           Alarms         39           Triggered alarms         39           Defined alarms         40           Alarm action library         41           5. Traffic Log         43           Overview         43           Designed interval data         44           Log ed interval data         44           Log ed interval data         45           6. Alarms	Overview	17
Switching network traffic view         18           Detaching a tab to a window         19           Collapsing and resizing a table column         20           Changing the data in the charts         20           Sorting a table column         22           Searching for network traffic details         22           Filtering network traffic details         23           Viewing more detail         24           Exporting network traffic data         24           Protocols         25           Hosts         27           Conversations         28           Protocols per host         30           Protocols per conversation         32           Network cards         34           Network card conversations         36           Network         38           Alarms         39           Triggered alarms         39           Defined alarms         40           Alarm action library         41           5. Traffic Log         43           Overview         43           Designed interval data         44           Log ed interval data         44           Log ed interval data         45           6. Alarms	Applet interface overview	17
Collapsing and resizing a table column       20         Changing the data in the charts       20         Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Doesn'ew       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50		
Changing the data in the charts       20         Sorting a table column       22         Searching for network traffic details       23         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50	Detaching a tab to a window	19
Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Adding alarms       47         Edit alarms       50	Collapsing and resizing a table column	20
Sorting a table column       22         Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Adding alarms       47         Edit alarms       50		
Searching for network traffic details       22         Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5 Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6 Alarms       47         Adding alarms       47         Adding alarms       47         Edit alarms       50		
Filtering network traffic details       23         Viewing more detail       24         Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50	Filtering network traffic details	23
Exporting network traffic data       24         Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50	Viewing more detail	24
Protocols       25         Hosts       27         Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50		
Conversations       28         Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50	Protocols	25
Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alding alarms       47         Edit alarms       50	Hosts	27
Protocols per host       30         Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alding alarms       47         Edit alarms       50	Conversations	28
Protocols per conversation       32         Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       40         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Network cards       34         Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50	Protocols per conversation	32
Network card conversations       36         Network       38         Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50	Network cards	34
Alarms       39         Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50		
Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50	Network	38
Triggered alarms       39         Defined alarms       40         Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Adding alarms       47         Edit alarms       50	Alarms	39
Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Alarm action library       41         5. Traffic Log       43         Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50	Defined alarms	40
Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Overview       43         Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Display logged statistics       43         Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Logged interval data       44         Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Log manager       45         6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
6. Alarms       47         Alarms       47         Adding alarms       47         Edit alarms       50		
Alarms       47         Adding alarms       47         Edit alarms       50		
Adding alarms		
Edit alarms50		
	Remove alarms	

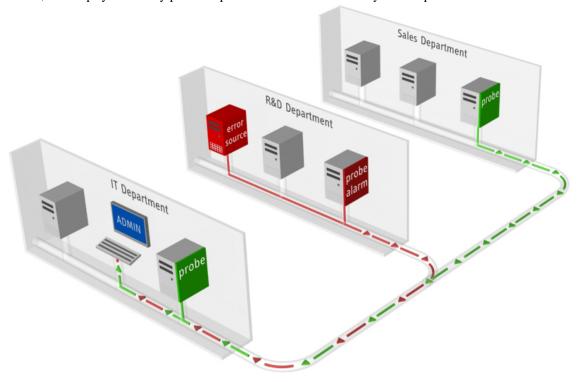
Alarm actions	52
E-mail alarm actions	52
Adding a e-mail alarm action	52
Edit e-mail alarm actions	54
Remove e-mail alarm actions	55
Alarm action library	55
7. Setup	57
Overview	57
Collected statistics	57
Reset interval	58
Network interface	59
Host name resolving	
Users and passwords	59
Filters	62
Ethernet address filters	62
IP address filters	62
Protocol filters	63
E-mail configuration	63
8. Advanced	
Manually starting the probe	65
Starting the stand-alone client	
Command line options	65
Resetting the admin password	66
Dump packet content to the console	67
Running the probe as a Windows service	68
Automatically starting the probe on *NIX	68
Configure web browsers to use Java (Linux)	
Starting the probe with no IP assigned to the interface	69
Performance tuning	70
9. Practical Use	71
Slow network	71
Monitoring	73

## **List of Tables**

2.1.	Supported brows	sers	7
4.1.	Filter operators		23

# **Chapter 1. Introduction**

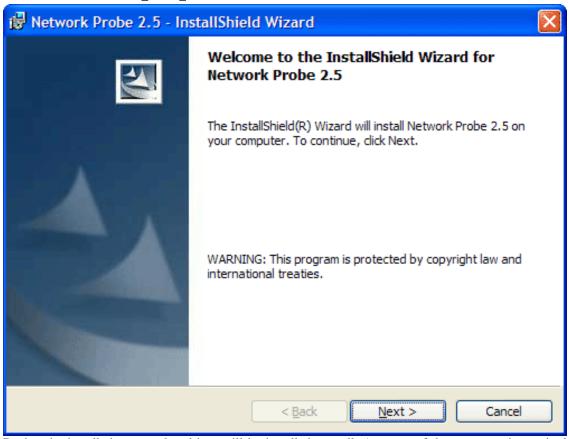
Network Probe is a network traffic monitor and protocol analyzer that gives you an instant picture of the traffic situation on your network. It displays detailed information about the type and amount of network traffic, and helps you identify potential problems and bottlenecks in your computer networks.



# **Chapter 2. Installation**

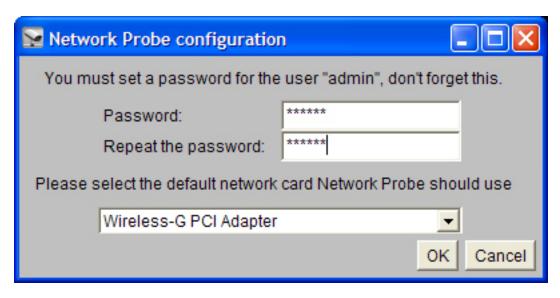
#### Windows installation

Double click the Network Probe 2.x-install.exe file and follow the instructions.



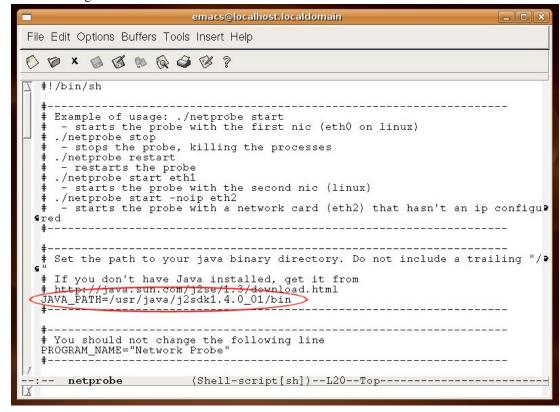
During the installation, a packet driver will be installed as well. A restart of the computer is required after installation is done, otherwise the packet driver won't start. The 2.x version will not overwrite any existing 1.x versions. If you have a 1.x version installed, you can copy the file "Program 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

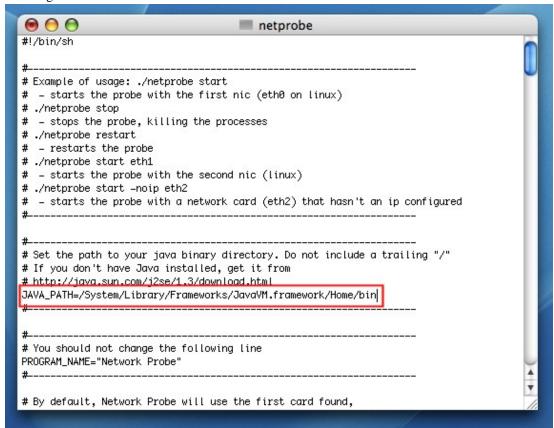
first time you start Network Probe, you will be asked to set a password for the admin user.

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 been 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 "/".



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".

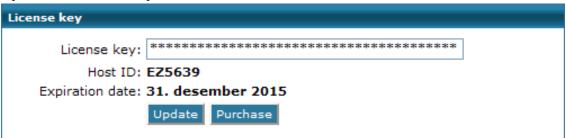
To keep configurations from older versions of Network Probe, copy the file "config.txt" from the con-

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

### License key



To enter the license key click on "Setup" and then on "Probe configuration". Enter the license key in the input field and click the "Update" button.



### **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):

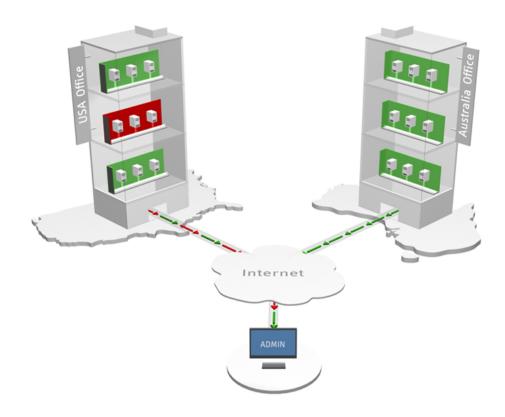


The computer should be connected to a mirrored port on your network switch, also known as a SPAN (Switched Port Analyzer) port. The normal operation of a switch is to send packets only to the computer they destinate to, but a SPAN port receives a copy of all packets going through the switch. A SPAN port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

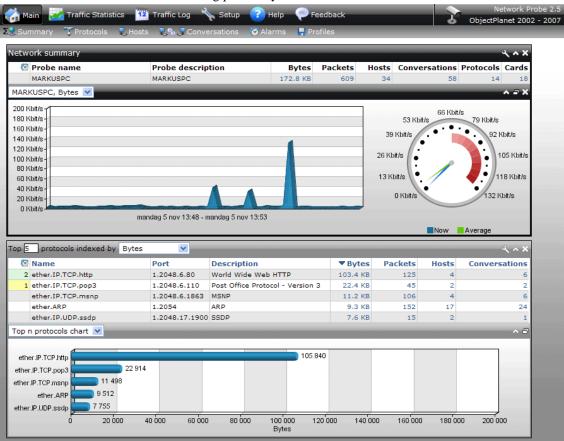
Platform	Browser	Version
Windows	Internet Explorer	6 and newer
Windows	Firefox	1.5 and 2.0
Windows	Opera	8.54
Linux	Firefox	1.5 and 2.0
Mac	Firefox	2.0

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 troughput, top protocols, hosts, talkers listeners and conversations taking place on your network.

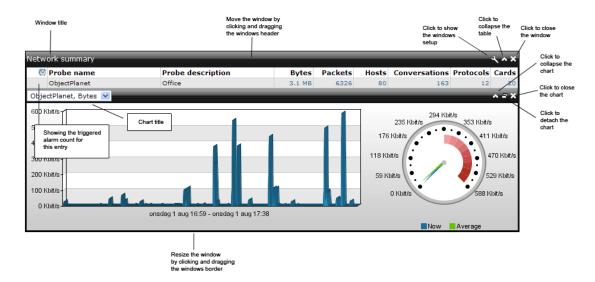


#### **Windows**

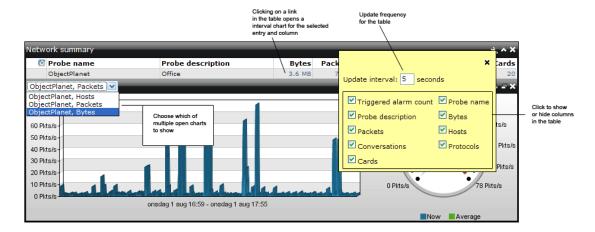
Show windows by clicking on the windows name in the top menu.



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.



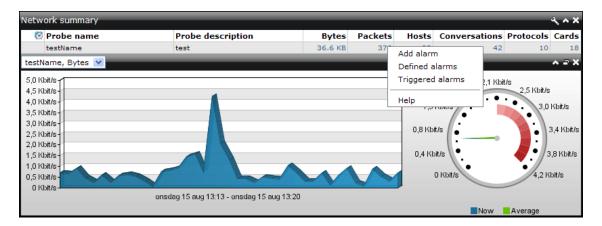
The table can be customized through the windows setup screen. Clicking links in the table opens an interval chart for the selected entry and column. Which of the multiple open charts to display can be choosen in the drop down box between the chart and the table. Interval charts are updated when there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



#### Window right click menu

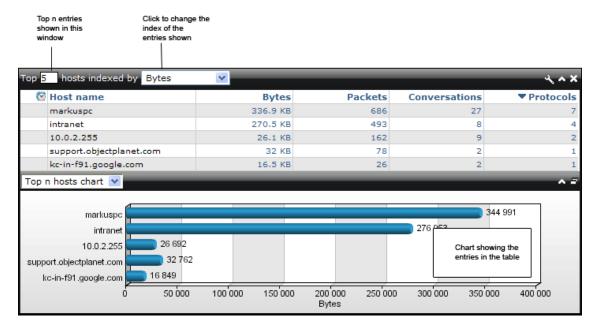
Each window has a right click menu which lets you manage alarms for the windows table.

- 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.

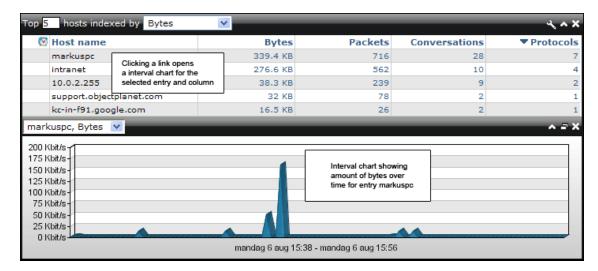


## Top n windows

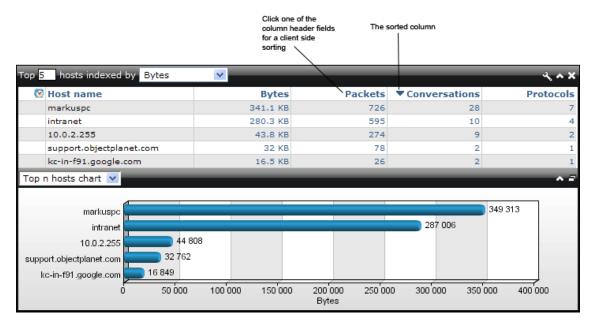
Using the top n windows you can watch the top n protocols, hosts, talkers, listeners and conversations on your network. Per default the top n data is indexed by the amount of traffic the entries have. You can change the index to the number of packets, the number of hosts, conversations or protocols. 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.

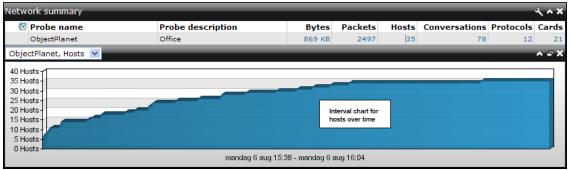


## **Summary window**

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.

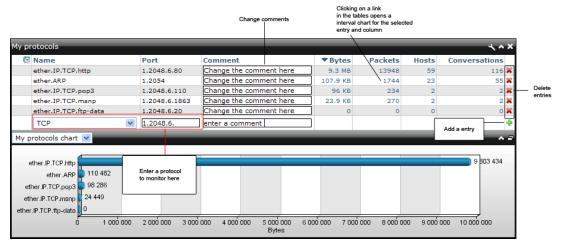


Interval charts for conversations, protocols and network cards are line charts and show the amount of conversations, protocols or network cards over time.



## **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**

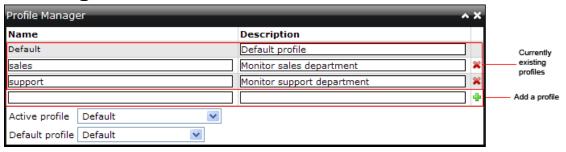
#### **Profiles**

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.

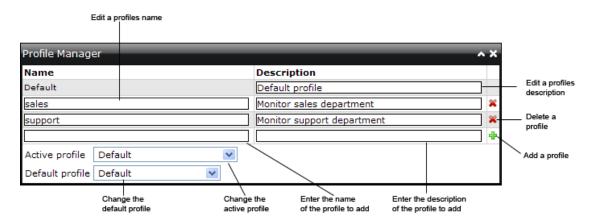
The default profile is the profile that is activated when a user logs on to the probe and can be changed in the "Profile Manager" window.

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.

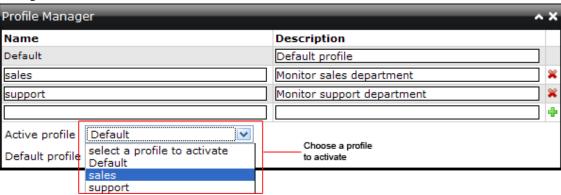


### **Switch profiles**

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".



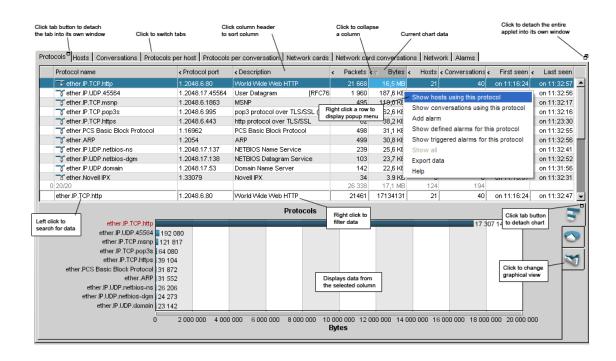
# **Chapter 4. Traffic Statistics**

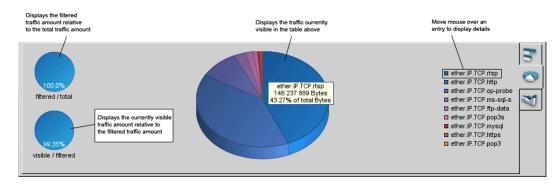
#### **Overview**

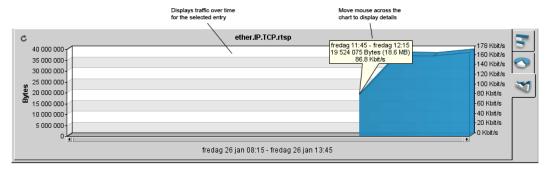
The Traffic Statistics screen lets you access live data. Show the Traffic Statistics screen by selecting the 'Traffic Statistics' button on the top of the window.



## **Applet interface overview**





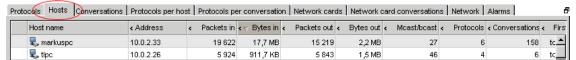


# Switching network traffic view

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

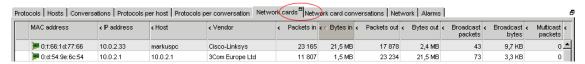


The hosts tab was clicked, and the view switched to the hosts table:

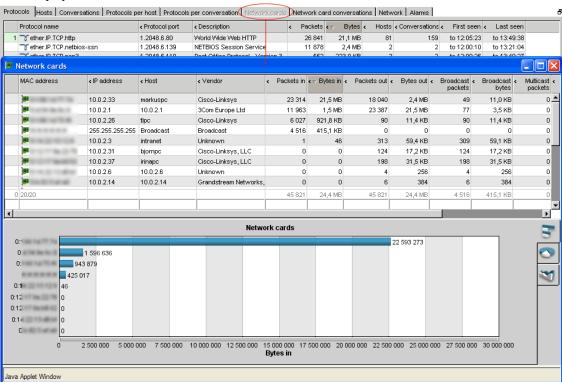


## Detaching a tab to a window

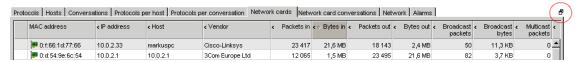
You can detach a tab into its own top-level window by doing a right-click on the tab, or clicking the tab detach button that appears when you move the mouse over the right edge of the tab. This enables you to see more than one type of network statistics at the same time as well as giving you the possibility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



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

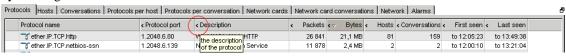


You can also click the detach button located at the top right to detach the entire main application window. This enables you to resize the application while at the same time having all the views inside one window frame.

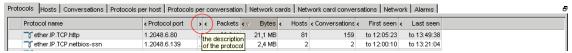


## Collapsing and resizing a table column

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.

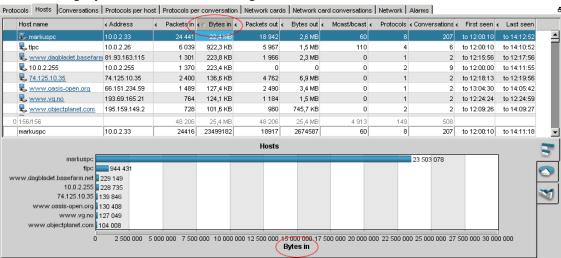


A column is made visible again by clicking the same arrow, now pointing to the right in the collapsed column header.

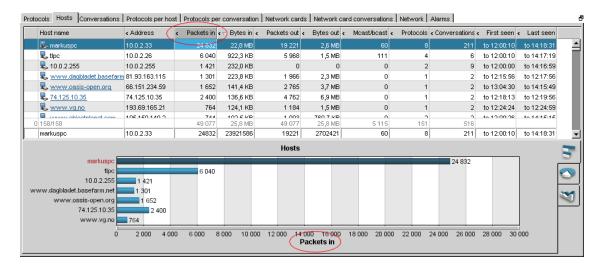


### Changing the data in the charts

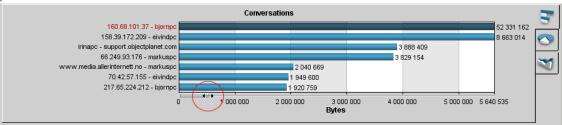
The data displayed in the bar chart and pie chart is the amount from the currently selected column, indicated with a slightly darker column header background.



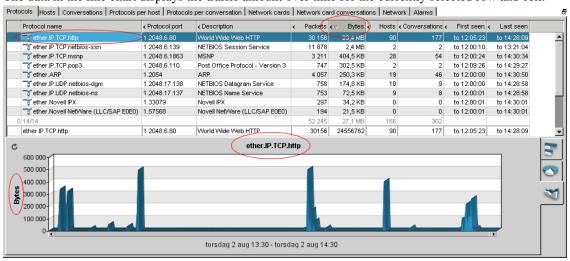
The data can be changed by selecting a cell from another column. Only data from numerical columns can be visualized in the bar chart. You can also change the selected column by typing the left or right key on your keyboard.



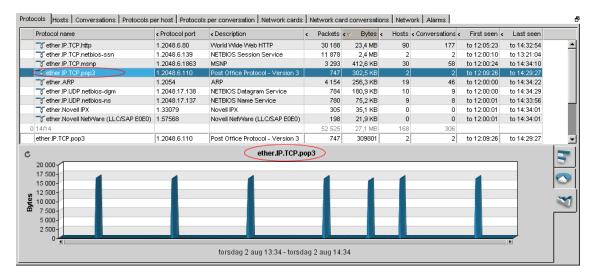
The range of the chart can be adjusted by dragging the range adjuster placed at the bottom of the chart, just above the axis values.



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

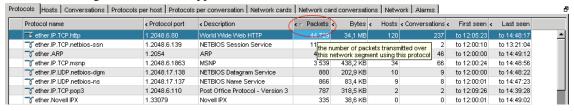


Change the data in the line chart by selecting another row in the table.



### Sorting a table column

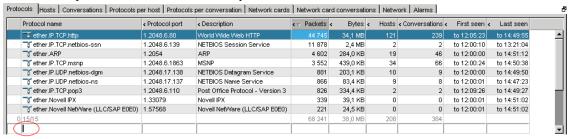
Left click a table's column header to sort the selected column. Textual columns are sorted in ascending order while numerical columns are sorted in descending order with the largest value at the top. Click the column header again to sort in the opposite order.



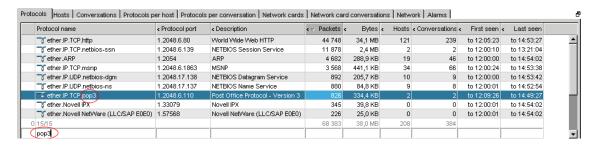
The currently sorted column will have a sort order indicator visible in the column header, indicating which order the column was sorted in.

## 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.



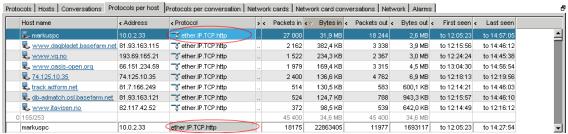
The phrase 'pop3' was typed in the first field of the filter bar, and the ether.IP.TCP.pop3 protocol was found in the table.



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.

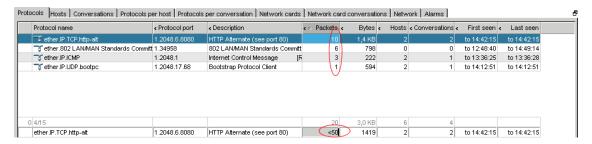


In the above image the user selected a row with the www-http protocol and right clicked the filter bar field for the protocol column to display only hosts that have used the http protocol since the probe started or was reset.

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.

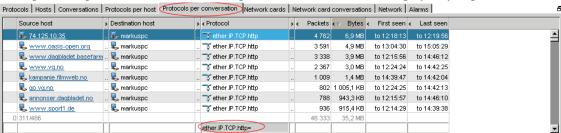


### Viewing more detail

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



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.

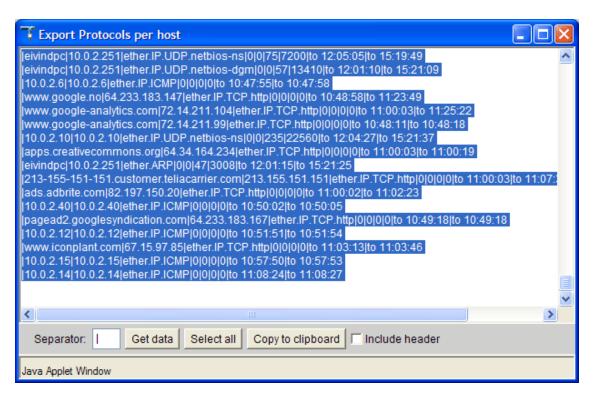


## **Exporting network traffic data**

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



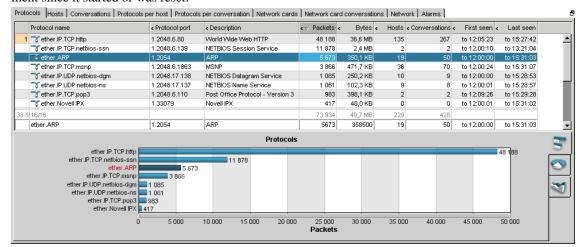
When you select 'Export data' a window is opened containing all the data in the table in a text area which you can use to copy and paste the data. The data in the window is exactly the same data as in the table with the correct sorting, filter settings, and visible columns.



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 poup menu is displayed if you right click a protocol entry.

Show hosts using this protocol

Show conversations using this protocol

Add alarm

Show defined alarms for this protocol

Show triggered alarms for this protocol

Show all

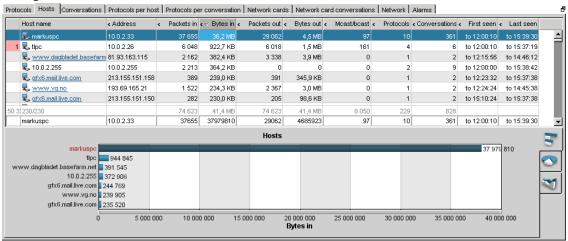
Export data

Help

- 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 buy 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 poup 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

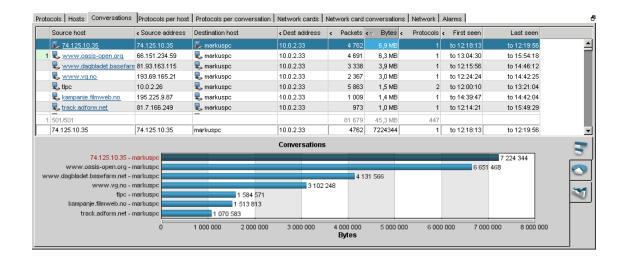
Export data

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 buy 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 poup 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

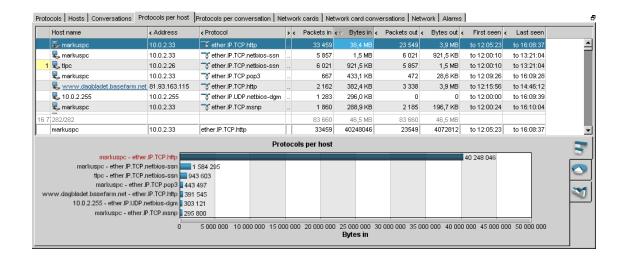
Export data

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 poup 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

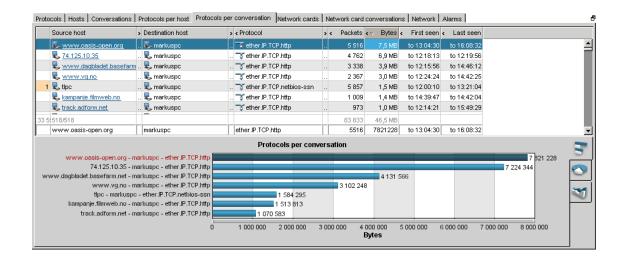
Help

- 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 occured. 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 poup 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

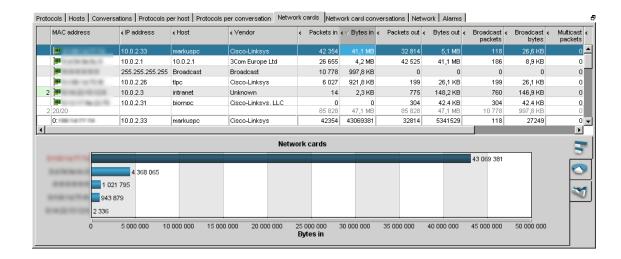
Help

- 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 poup menu is displayed if you right click an entry.

Show this vendor only

Show source conversations for this card

Show destination conversations for this card

Add alarm

Show defined alarms for this card

Show triggered alarms for this card

Show all

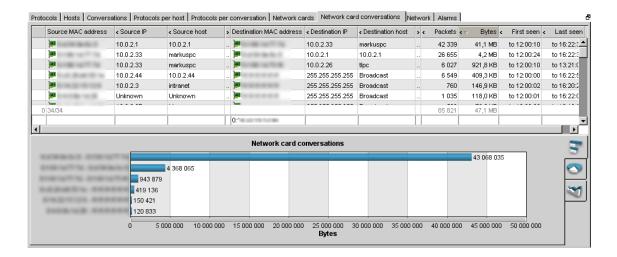
Export data

Help

- **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

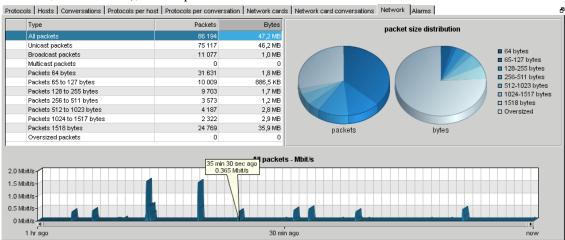
The network card conversations poup menu is displayed if you right click an entry.

Add alarm
Show defined alarms for this card conversation
Show triggered alarms for this card conversation
Show all
Export data
Help

- 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 poup menu is displayed if you right click an entry.

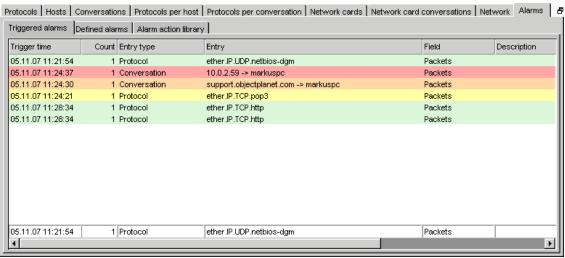
Add alarm
Show defined alarms for this entry
Show triggered alarms for this entry
Export data
Help

- 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**

### **Triggered alarms**

The triggered alarms displays information about the alarms that have been triggered sinde the probe started or was reset.

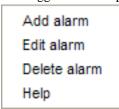


- Trigger time displays the time when the alarm was triggered
- Count the trigger count for the alarm
- Entry type the table the alarm is for.
- Entry the entry the alarm is for.
- Field type the alarm is triggered based on this fields value.
- **Description** the description set for the alarm.

- Value the value which caused the alarm to be triggered.
- **Severity** the severity of the alarm.

#### Triggered alarms popup menu

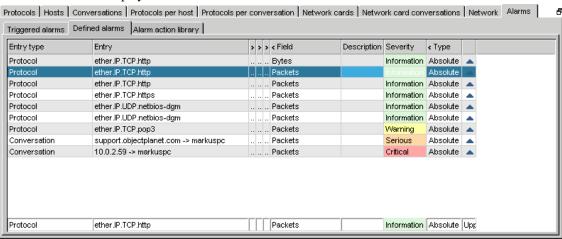
The triggered alarms poup menu is displayed if you right click an alarm entry.



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

### **Defined alarms**

The defined alarms displays information about the defined alarms.



- Entry type the table the alarm is for.
- **Entry** 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** the severity of the alarm.
- Type the type of the alarm (Absolute, Delta).

#### Defined alarms popup menu

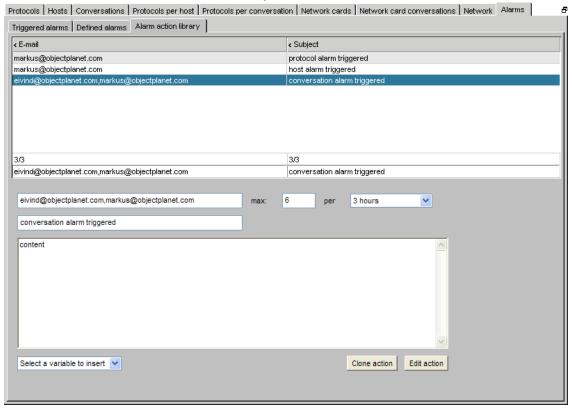
The defined alarms poup menu is displayed if you right click an alarm entry.



- Add alarm- this will let you add a alarm.
- Edit alarm this will let you edit the clicked alarm.
- **Delete alarm** deletes the clicked alarm entry.

### **Alarm action library**

This tab shows all the actions in the action library. Actions can also be added, edited or removed.



- E-mail the recipients of the e-mail to send.
- Subject the subject of the e-mail to send.

#### Action library popup menu

The action library poup menu is displayed if you right click an action entry.

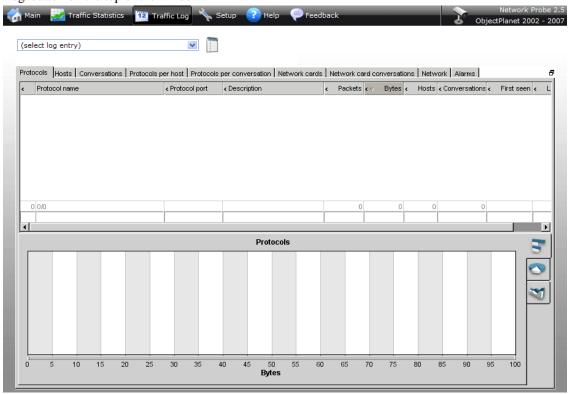
Delete action Help

• **Delete action-** deletes the action.

# 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.

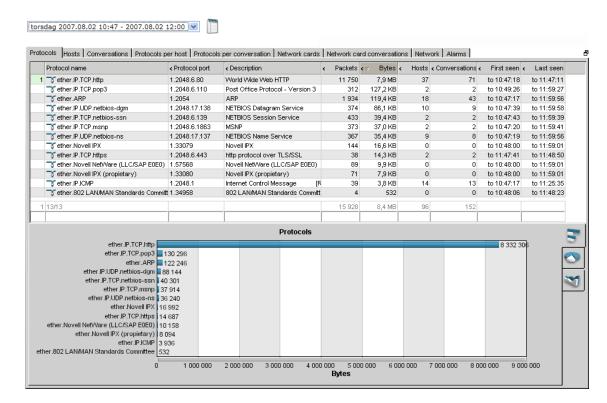


# **Display logged statistics**

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.

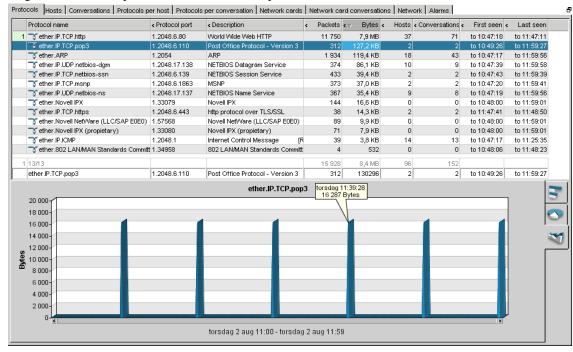


The network statistics from the selected time period will then be displayed in the network probe applet, and all the normal operations work as with the live data.



# Logged interval data

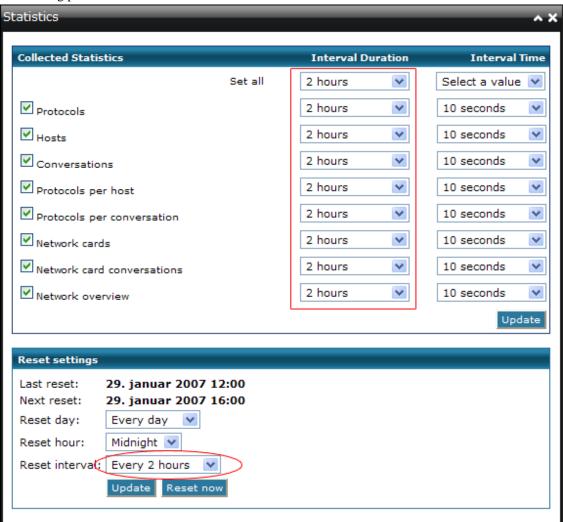
The interval data displayed for the logged data might not match the period of the log selection, but is the length of the interval period set in the Probe setup.



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.



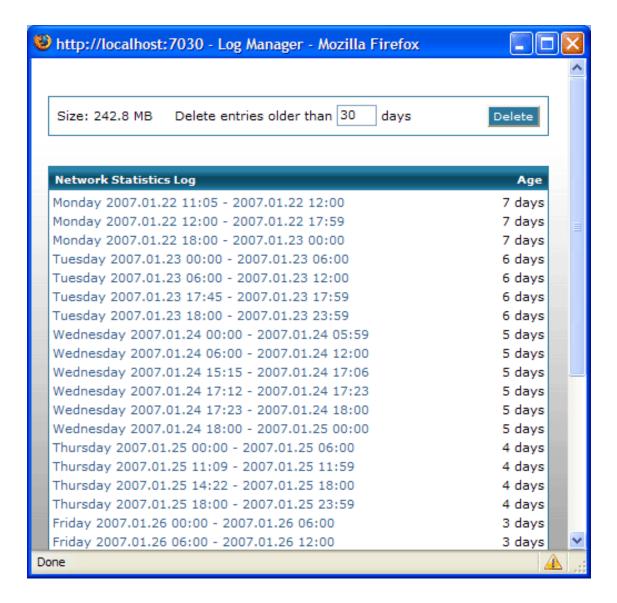
# Log manager



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.



# 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**

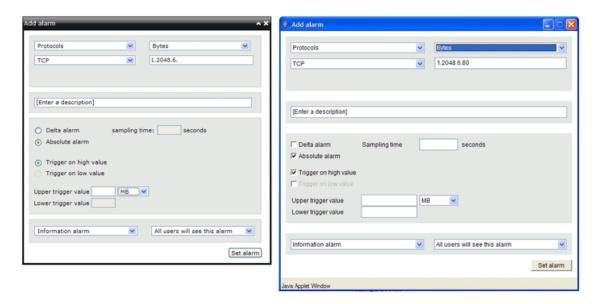
A delta alarm is triggered when the monitored entries delta value for the given field is larger than a specified value. For each sampling time there is taken a sample of the monitored entries value for the given field. If the difference of the two last samples taken is larger than the specified trigger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

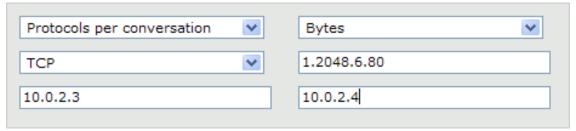
# **Adding alarms**

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".



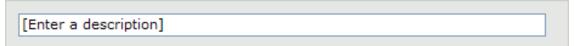
#### **Entry**

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).



#### **Description**

Optionally you can add a description for the alarm.



#### Alarm and trigger type

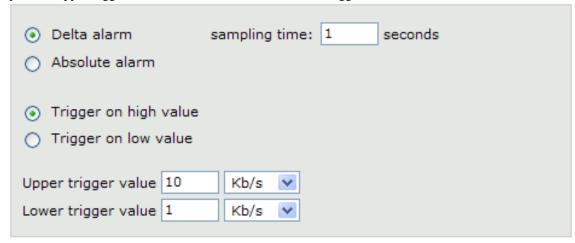
Choose whether you want the alarm to be an absolute or delta alarm. If you choose delta alarm you will also need to enter a sampling time.

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.

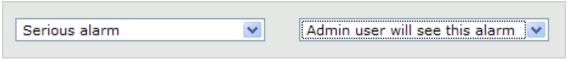
The below image shows setting a delta alarm with sampling time 1 second. The trigger type is set to up-

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

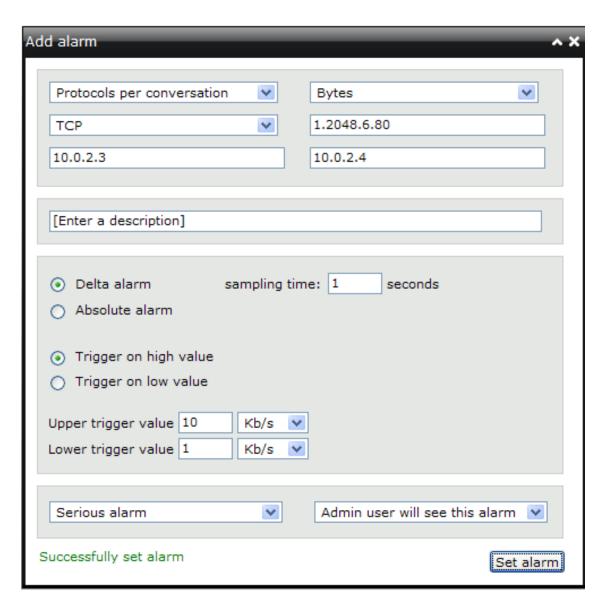


#### Severity and Visibility

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.



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



### **Edit alarms**

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

#### Main

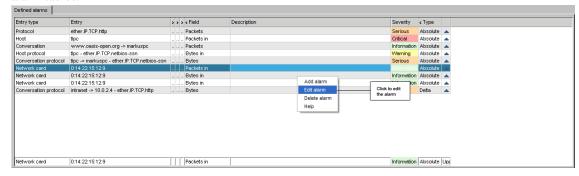
In the Main screen, alarms can be edited by clicking the edit icon to the right of the alarm in the alarm windows, or by choosing "Edit alarm" from the right click menu in the alarm windows.



#### **Traffic Statistics**

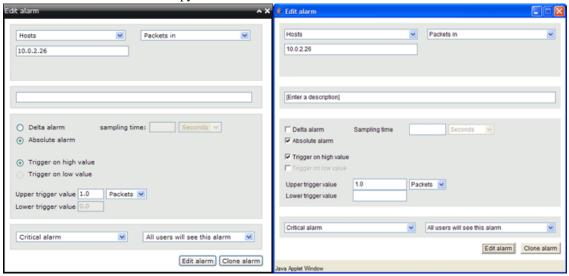
In the "Traffic Statistics" alarms can be edited by choosing "Edit alarm" from the right click menu in the

#### alarm tables.



#### 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.

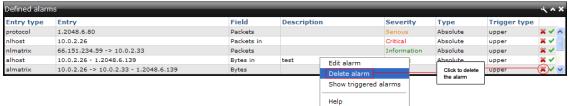


### Remove alarms

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

#### Main

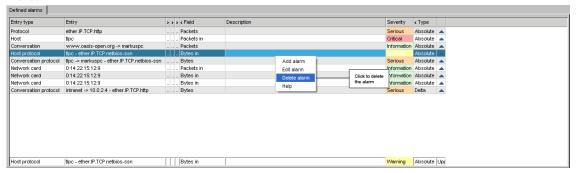
In the "Main" tab alarms can be removed by cliking on the delete icon to the right of the alarm in the alarm windows, or by choosing "Delete alarm" in the right click menu.



#### **Traffic Statistics**

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

#### menu.



### **Alarm actions**

### E-mail alarm actions

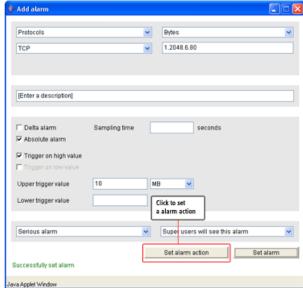
When a alarm is triggered you can set up Network Probe to send a given e-mail. Before any e-mails can be sendt Network Probes email server needs to be set up. You can specify any number of emails to be sendt when a alarm is triggered. To not fill up your inboxes you can specify how often a email will be sendt on a given time period. Frequently sendt e-mails can be added to the action library. Later on actions from the action library can be added to multiple alarms.

The e-mails sendt by Network Probe are fully configurable. A single or multiple recipients can be set, the subject and the content can be set. In the content of e-mail variables from the triggered alarm can be inserted.

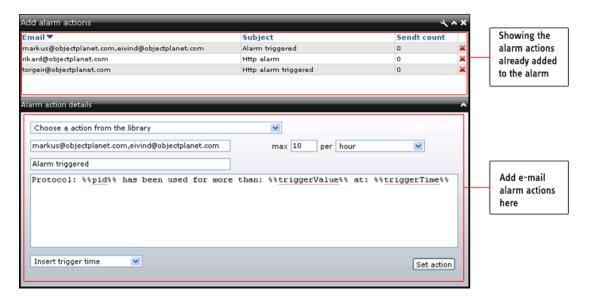
### Adding a e-mail alarm action

Alarm actions can be added from both the "Main" and the "Traffic Statistics" tab. In both cases alarm actions are set by clicking the add "Set alarm action" button in the add alarm window.

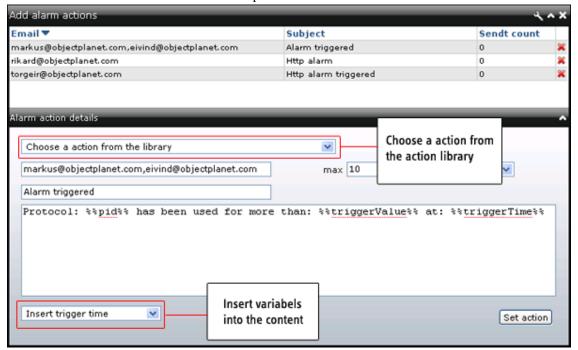




Adding alarm actions is done in a new window. The "Add alarm actions window" The top half of this window shows a table containing the e-mail alarm actions already added to this alarm. In the bottom part of the window e-mail alarm actions can be added.



To add a e-mail alarm action enter the recipient address, the subject and the content. Also specify how many of this e-mails can maximum be sendt in a given time interval. You can also choose a action from the action library. A e-mail can be sendt to multiple recipients by entering multiple e-mail addresses comma separated in the recipients field. Variables such as trigger time and trigger value can be inserted into the content of the e-mail. Variables are replaced with their value when the e-mail is sendt.

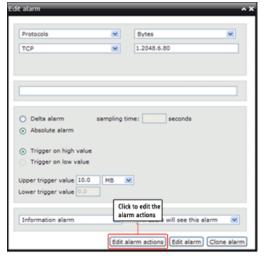


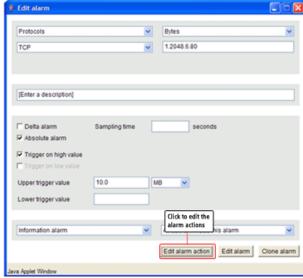
When a e-mail is sendt all the variables in the content are replaced with their values. In addition to the content the triggered alarms is added to the content of the email.

```
Protocol: 1.2048.6.80 has been used for more than: 10.1 MB at: 2007.11.05 09:34:50
<alarm>
        <triggerValue>10.1 MB</triggerValue>
        <triggerTime>2007.11.05 09:34:50</triggerTime>
        <triggerCount>1</triggerCount>
        <defined>
                <id>4</id>
                protocol
                <src></src>
                <dst></dst>
                <pid>1.2048.6.80</pid>
                <counterId>1</counterId>
                <upperTriggerValue>10.0</upperTriggerValue>
                <lowerTriggerValue>0.0</lowerTriggerValue>
                <samplingTime>1</samplingTime>
                <description></description>
                <severity>0</severity>
                <absoluteAlarm>true</absoluteAlarm>
                <triggerType>upper</triggerType>
                <upperUnit>MB</upperUnit>
                <le><lowerUnit>MB</lowerUnit>
                <visibility>0</visibility>
        </defined>
</alarm>
```

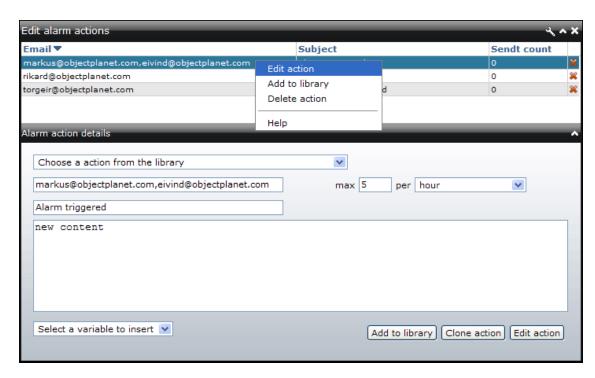
### Edit e-mail alarm actions

E-mail alarm actions can be edited in both the "Main" and "Traffic Statistics" tab by clicking the "Edit alarm action" button in the "Edit alarm" window.



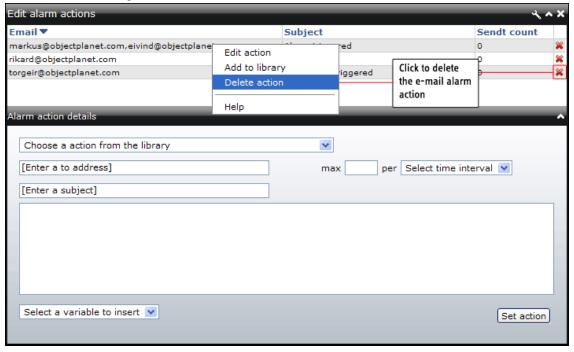


Click a e-mail alarm action in the action table or choose "Edit action" in the right click menu to select a e-mail alarm action. Once the action is selected the actions details are shown in the bottom "Alarm action details" section of the window. Here the action can be edited. Confirm any changes by clicking the "Edit action" button. Click the "Clone action" button to clone the action. By clicking "Add to library" the e-mail alarm action is added to the action library.



### Remove e-mail alarm actions

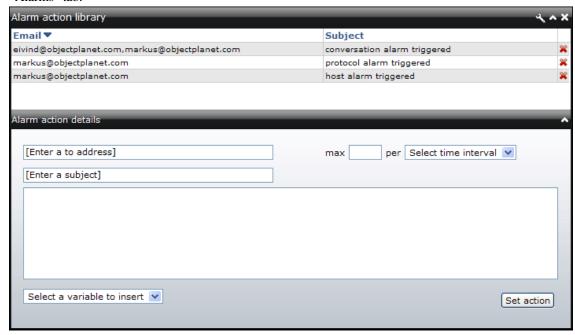
E-mail alarm actions can be removed by clicking the remove button in the actions tables or choosing "Delete action" from the right click menu.



# **Alarm action library**

The alarm action frequently used actions can be stored for later use. Later on the actions in the library can be added to multiple alarms. The alarm action library can be accessed from the "Main" and the

"Traffic Statistics" tab. In the "Main" tab the action library can be accessed by clicking "Alarm action library" from the "Alarms" top menu. In the "Traffic Statitistics" tab you can find action library under the "Alarms" tab.

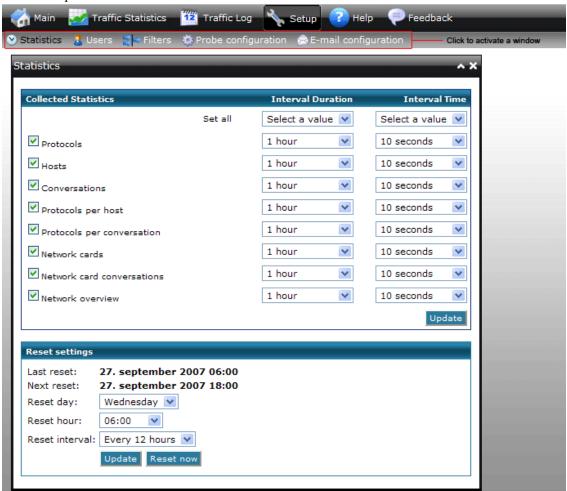


In the action library action can be added, edited or removed the same way as in the Add/Edit alarm actions windows.

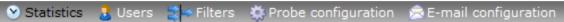
# Chapter 7. Setup

### **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.

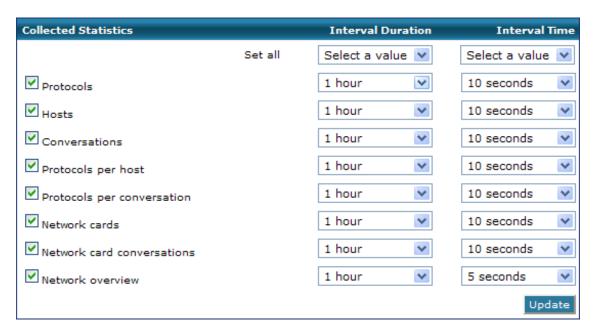


### **Collected statistics**



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 comsume a lot of memory on large networks.



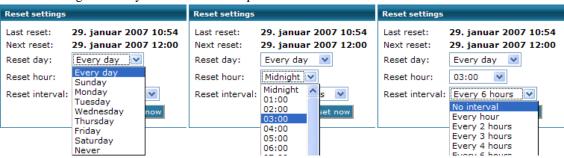
### Reset interval



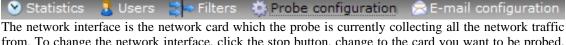
This displays the times the network traffic statistics are reset. By default the probe is reset every day starting from midnight and every sixth hour. None of the statistics entries are removed when the probe is reset, but their counters values are set to 0. Entries with no traffic since the last reset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



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



### **Network interface**

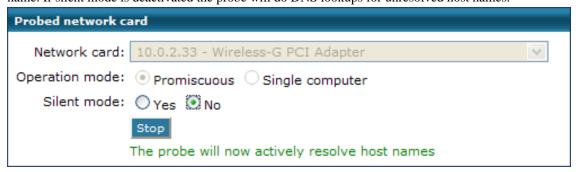


from. To change the network interface, click the stop button, change to the card you want to be probed, then click the start button. Uncheck the "Promiscuous" box if you want to start the probe in non-promiscuous mode. In non-promiscuous mode only traffic going from/to the probing computer will be picked up, as well as broadcast/multicast traffic.



# Host name resolving

Network Probe uses the DNS packets on the network probed, to resolve host names. In silent mode the probe does not generate any DNS lookup itself, but tries to decode DNS packets to get the correct host name. If silent mode is deactivated the probe will do DNS lookups for unresolved host names.



# **Users and passwords**

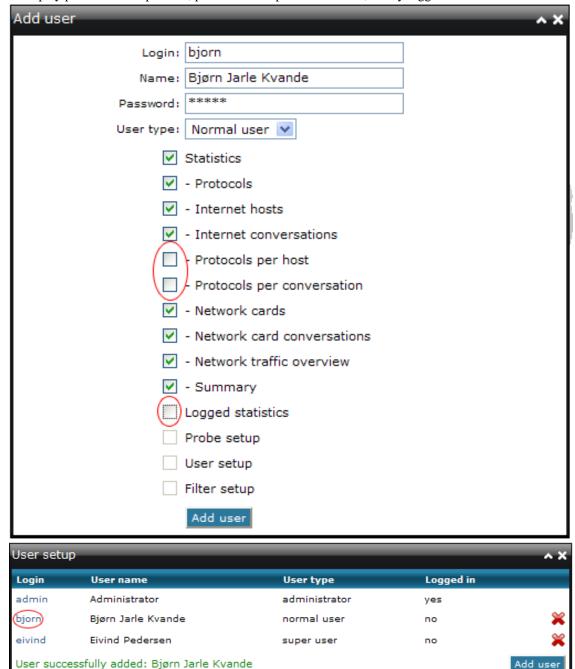


The default user configured for the probe is the Administrator. You can add additional users to the probe having restricted access to the network statistics data and probe setup. Only administrators and super users can access the user setup.

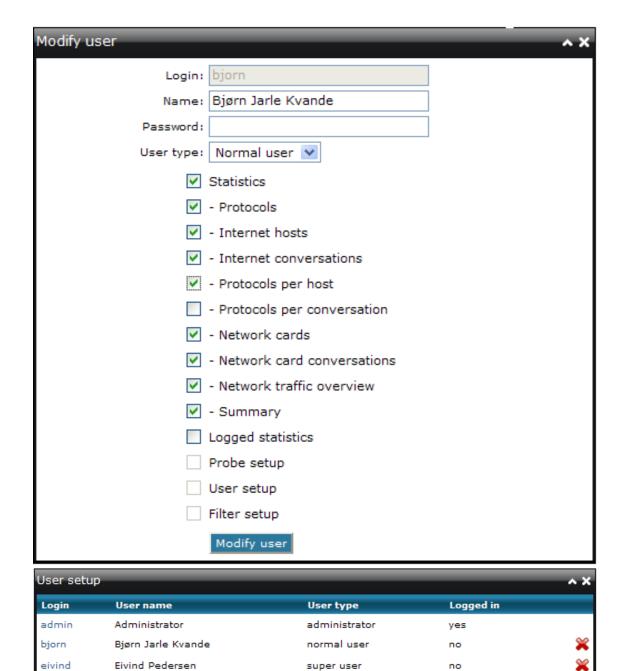


You can add a new user by clicking the 'Add user' button. The below image shows adding the new user

'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.



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.



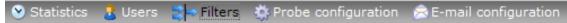
Delete a user by clicking the delete button to the right for the user. In the below image the user bjorn has been deleted.

Add user

User successfully modified: bjorn



### **Filters**

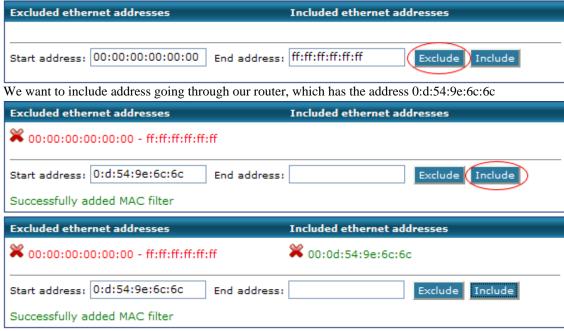


Filtering out some network traffic reduces the memory consumption, and makes it easier to monitor specific hosts or ports. By default there are no filter rules defined, and all traffic will be picked up.

### Ethernet address filters

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

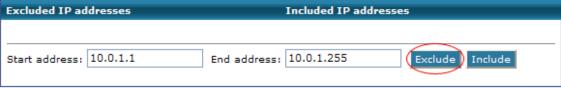
You can filter traffic on specific network cards or ranges of network cards, by adding the ethernet (MAC) address. For a single network card, add the ethernet address in one of the fields. For a range, add the start and stop address. The below image shows how to exclude all traffic.



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

### IP address filters

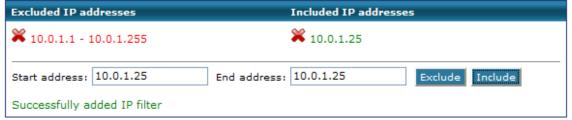
You can add a new IP filter rule by defining the start IP and end IP (a range). If it's only a single IP address, let start and end have the same value. Valid IP addresses are from 0.0.0.0 - 255.255.255.255. The below image shows adding the new IP exclusion rule, 10.0.1.1 - 10.0.1.255.



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



These are the filter rules defined so far:



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

### **Protocol filters**

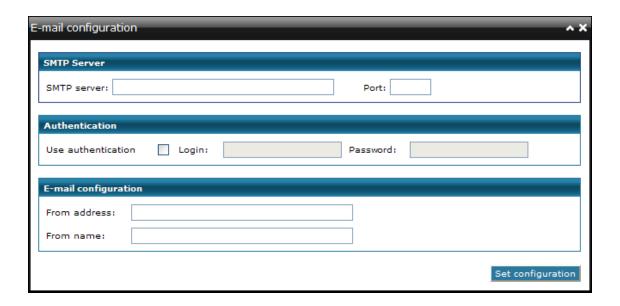
Filter rules for protocols/port numbers can be set the same way: Choose the protocol type (TCP, UDP, IP or Ethernet), the port number range and click the 'Include' or 'Exclude' button. The example below shows that all TCP traffic going on port 1 - 200 is never picked up by the probe, except TCP traffic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



### E-mail configuration



Before any e-mails can be sendt out the e-mail configuration needs to be set. You need to enter the SMTP server to use and the address e-mails are to be sendt from. If no port for the SMTP server is entered the standard port, which is 25, is used. In addition to the from address a from name can be set. If your SMTP server requires authentication to send e-mails check the "Use authentication" checkbox and enter the login and password to use.



# **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 adapeter 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 the 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 usefull 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.arpa.....
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.arpa....?..
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.....
```

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
```

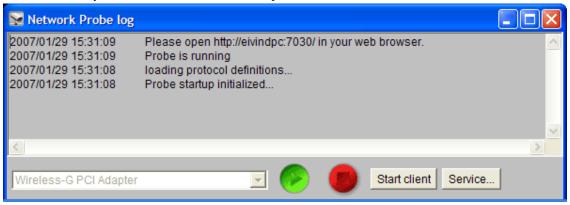
1 is for ethernet, 2048 is IP (0x800), 6 is for TCP, and 80 is the HTTP port number.

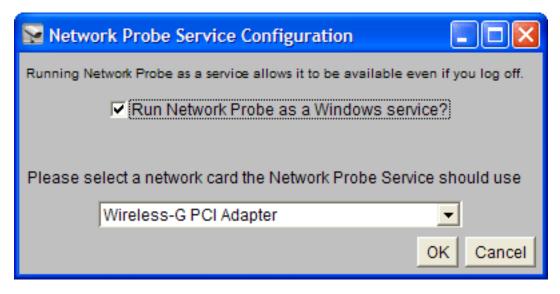
This will dump all the HTTP traffic for the host with IP 10.0.1.20:

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 (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 libjava (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
```

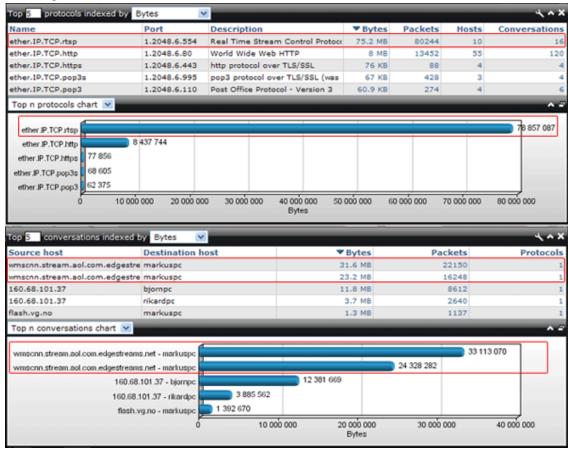
Heavy CPU usage is normally caused by the chart generation process, when there are many intervals.

# **Chapter 9. Practical Use**

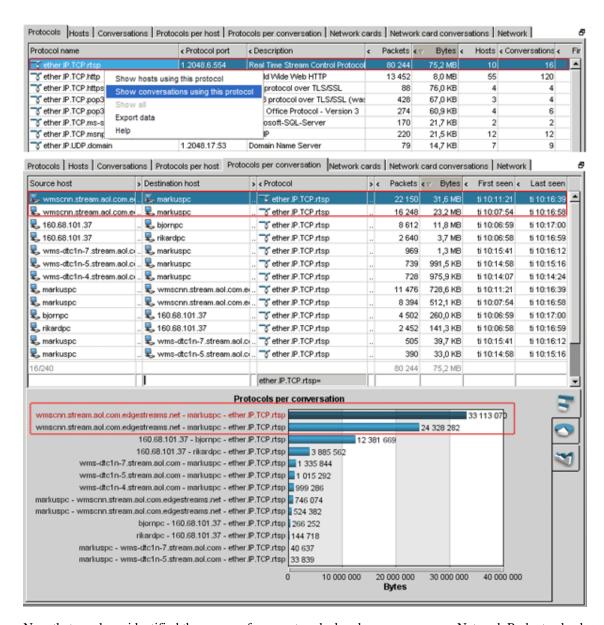
### Slow network

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.

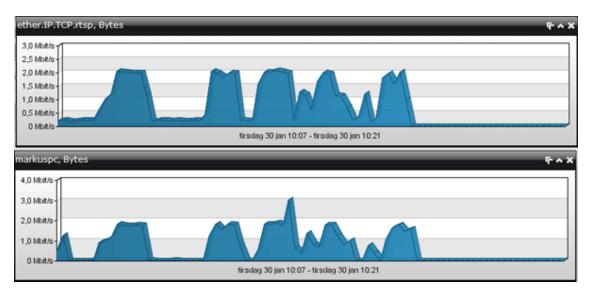
In the top protocols window you can see that rtsp is using a substantial part of the bandwidth. In the top host window you can see that markuspc is using the most bandwidth, and in the top conversations window you see that markuspc has two conversations with streams from cnn. Markuspc is most likely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

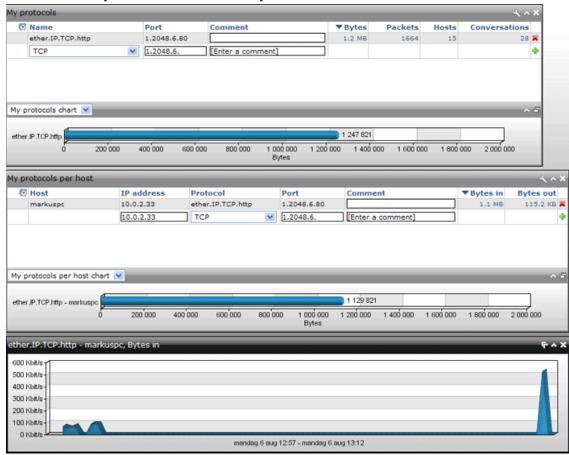


Now that you have identified the source of your network slowdown, you can use Network Probe to check if the host markuspc actually stops watching videos on cnn. To do this you can detach the interval chart for rtsp in the top protocols window, and the interval chart for markuspc in the top hosts window.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

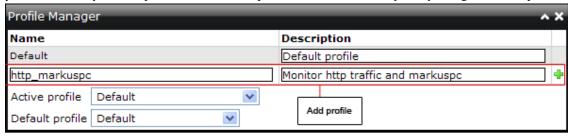


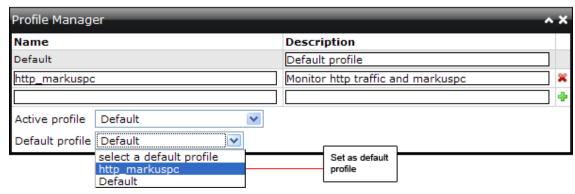
# **Monitoring**

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 procotols per host" window. Open the "My procotols per host" window and enter markuspc and 1.2048.6.80, also you could detach the byte interval chart for this entry.

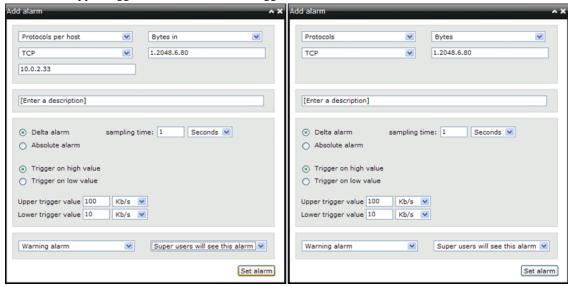


Now create a new profile, name it for example http\_markuspc. The profile saves the layout of the Main screen. Later on you can easily activate the profile and monitor the http protocol and host markuspc. If you set the newly created profile as the default profile it is activated everytime you log on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



To automatically let Network Probe notify you when one of the alarms goes of a e-mail alarm action can be used. By adding a e-mail alarm action a email is sendt everytime the alarm is triggered. The below image shows adding a e-mail alarm action. For more information on how to add e-mail alarm actions click here.

