

MaaTec Network Analyzer 1.6



Table Of Contents

1	Installation Guide	1
2	Quickstart	2
2.1	Starting MTNA	2
2.2	Network Statistics	2
2.3	Load over Time Statistics	5
2.4	Collecting Packets	7
2.5	Analyzing Data	7
2.6	Printing and Copying	9
2.7	Packet Filtering	9
2.8	Saving and Loading Data	11
2.9	Main Window Overview	13
3	Advanced Features	15
3.1	Generating Reports	15
3.2	Advanced Report Topics	17
3.3	Coloring the List View	20
3.4	Scheduled Packet Capturing	20
3.5	Customizing the Application	21
3.6	Modifying the configuration files	22
3.7	Saving and Loading your Settings	23
3.8	System Performance and Packet Loss	23
4	More Help	25
5	Reference	26
5.1	Main Window	26
5.1.1	Packet Sources Window	26
5.1.2	Packet Source View	27
5.1.3	Packet Sink View	28
5.1.4	Packet List View	29
5.1.5	Decode View	31
5.1.6	Hex View	32
5.1.7	Scheduled Capture View	33
5.1.8	Statistics View	34
5.1.9	Load over Time Statistics View	35
5.1.10	Report View	36
5.2	Dialogs	36
5.2.1	Settings Dialog	36
5.2.2	Customize Dialog	57
5.2.3	File Properties Dialog	64
5.2.4	Edit Address Information Dialog	64
5.2.5	Color Selector	65
5.2.6	Register MTNA Dialog	65
5.2.7	About Box	66

5.3	Menus.....	67
5.3.1	File Menu	67
5.3.2	Edit Menu.....	69
5.3.3	Collect Menu.....	70
5.3.4	View Menu	70
5.3.5	Tools Menu	71
5.3.6	Window Menu	72
5.3.7	Help Menu	72
5.4	Toolbars	73
5.4.1	Standard Toolbar	73
5.4.2	Packet List Toolbar	74
5.5	Documents and Views.....	74
5.6	Packet List Columns.....	74
5.7	Statistics Modules	77
5.8	Load over Time Charts.....	79
5.9	Report Charts	83
5.10	Data Flow	85
5.11	Capture Filter.....	86
5.12	View Filter.....	86
5.13	Address Filter	87
5.14	Address Filter Examples	88
5.15	Address Filter Tips	89
5.16	Address Name Formats	90
5.17	Address Groups	91
5.18	Protocol Filter	92
6	Registration	94
7	Index	95

1 Installation Guide



You have two ways to install and uninstall the Network Analyzer application. The recommended way is to use the MTNA setup file that uses the Windows Installer. While the MaaTec Network Analyzer will run without rebooting your system, the Windows Installer setup may need a reboot for its own system files. So if you need to install the application without rebooting, or if you cannot use the Windows Installer (e.g. Windows NT 4 without Service Pack 6), you should follow the manual installation instructions below.

Installing and uninstalling MTNA with the MTNA setup file


Unzip the setup files, run Setup.exe, and follow the instructions. You can delete the setup files afterwards. The setup will add an entry in the Windows start menu (Programs > MaaTec > Network Analyzer).

To uninstall the application, open the control panel, double-click Add/Remove Programs (Vista: Programs and Features), select the MaaTec Network Analyzer entry, and click the Add/Remove button. In the remove/repair dialog choose the remove option and click Finish.

Installing and uninstalling MTNA manually

Create a directory for the MTNA files and unzip them into this directory. Now run the Mtna.exe file (see also Starting MTNA). The first time you run the application, you will be asked for a directory for the MTNA settings files. You will need to manually remove this directory when uninstalling the application. To uninstall the Network Analyzer, run the MTNA.exe file from the command prompt or via the Run command in the start menu with the /Unregister command line option (e.g. "C:\Program Files\MaaTec\MTNA.exe" /Unregister). This will clean up the registry. Now you can delete the application directory and the settings directory.


Switching the demo mode

The Network Analyzer can be licensed as standard (Std) and as Pro version. To check, which version fits your needs best, you can switch the trial version of the Network Analyzer between the Std-Demo and Pro-Demo mode: Open the About Box via the help menu or with the question mark button  in the toolbar and use the corresponding 'Switch to ...' buttons. You will need to restart the application to run the new demo mode. The features that are only available in the Pro version of the Network Analyzer are marked with (PRO VERSION) below the topic title inside the documentation.


2 Quickstart

2.1 Starting MTNA



 To start the Network Analyzer and to collect network data, you will need to use a Windows account with administrative credentials. You may run the application without these credentials, but you won't be able to access the network in this case.

If you are logged on as an administrator or if you are using Windows 98 or ME, you can start the Network Analyzer as usual. The full setup will have added a menu entry under MaaTec to your Start menu.

 If you are using Windows NT or Windows 2000, you need to log on as administrator to collect network data.

If you are using Windows XP, Windows 2003, or Windows Vista, you can use the 'Run as' command if you not have logged on as administrator. Right-click on the Network Analyzer entry in the start menu and choose 'Run as'. This will also work in the Windows Explorer or with desktop shortcuts. In the 'Run as' dialog choose an administrative account, enter the password, and click OK.




If you did not use the setup to install the Network Analyzer and this is the first time you start it, you will be prompted for a settings directory where MTNA will store its application data. Click the OK button to use the suggested directory.

2.2 Network Statistics

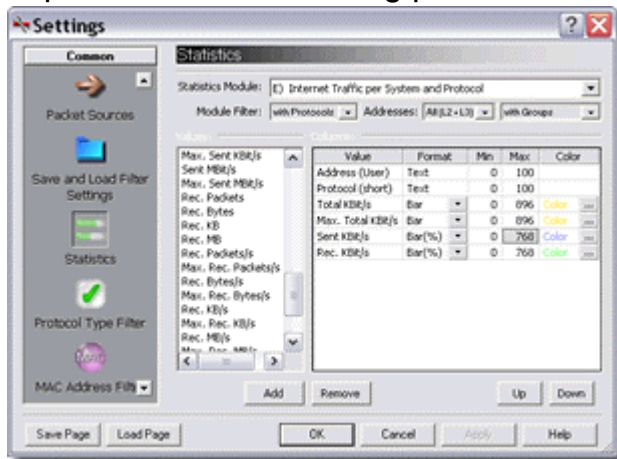


The MaaTec Network Analyzer offers two different network statistics views. The standard Statistics View is described here. It displays the current network load as well as the cumulated data volume and maximum network load per address, network card, protocol, connection, or a combination of these. This information is presented in a table based view as text, numerical values, or as horizontal bar graph.

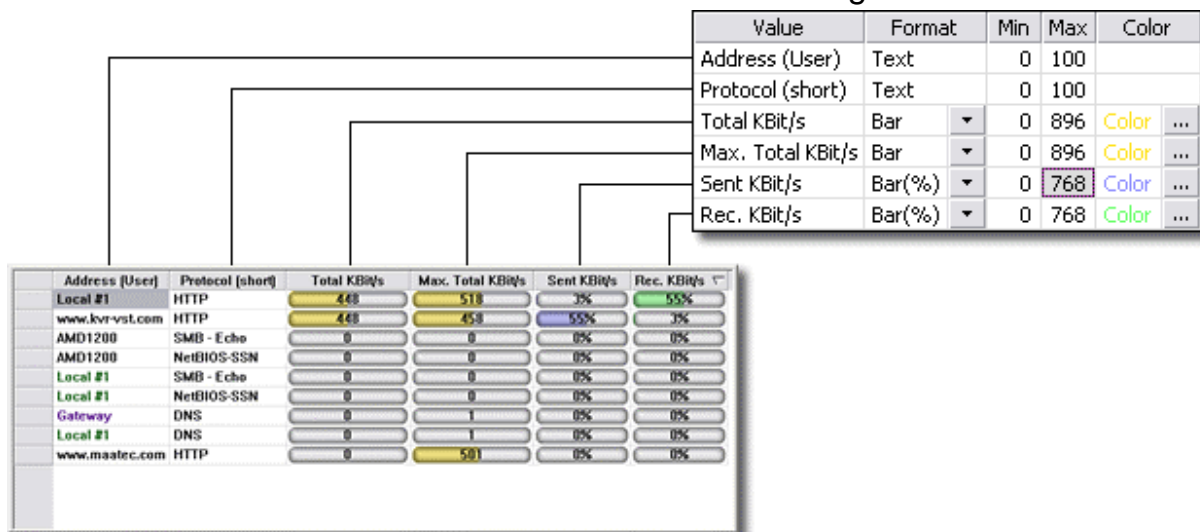
The Pro version of the Network Analyzer does also offer a Network Load over Time Statistics View. It presents the network load per address, protocol, etc. as line or bar chart with a history over a configurable period of time. The Load over Time Statistics are described in detail below.

You can use the Statistics View to view at different aspects of the data traffic in your network. Use the New Statistics toolbar button , the File > New Statistics menu command or press Ctrl+T on the keyboard to open the Settings dialog for the Statistics View. To change the settings for an open statistics view use the Collect > Capture Settings menu command.

Open the Statistics page of the Settings dialog. You can use the other pages in the dialog to configure filters that will restrict the packets that are evaluated for the statistics display. This works in the same way as the capture filter for collecting packets and is described in detail later on.



On the Statistics page you can choose between different statistics modules to analyze your network traffic. A detailed description of the different modules can be found on the Statistics Modules page. Select the statistics module 'Internet Traffic per System and Protocol' in group E) (if you switched off the Easy Statistics Mode in the Tools menu the module is called 'L3 Addr Higher Protocol Statistics'). This will fill the list on the left with the available display values (columns) for this module. The table on the right contains the chosen display values with some additional properties. Each of these values will be displayed in its own column in the Statistics View. This connection is shown in the image below.





To add more values, select one or more elements in the value list and click



the Add button. The new values will be added to the column list right after the currently selected item in this list. To remove items from the column list, select them and click the Remove button. To change the sequence of items in the column list, select one and use the Up and Down buttons to move the item up and down.



To get useful traffic graphs, you may need to modify the Max values of columns that are set to a graphic format (e.g. Bar). If you want to analyze a 10 MBit network, choose values that use MBit/s units and set the Max value to 10. If you want to look at traffic on a DSL connection, choose columns that use KBit/s units and set the Max value according to your connection speed (e.g. 768 for sent and received, and 896 for total data rates).



When your column list contains at least one address, one protocol, and one value column, click OK. This will create a new Statistics View that contains all selected columns.

 The Network Analyzer will usually start to collect data now. If the Auto-Start Collection option in the Tools Menu was disabled, you need to click the Start button  in the toolbar, use the Collect > Start menu command, or press F8 on the keyboard. If there is any traffic on your network, new data rows will be added to the view, displaying which address causes how much traffic using which protocol. You can sort the data by clicking on any column header. Clicking once will sort text columns in ascending order and numeric columns in descending order. If you click the header of a sorted column again the sorting order will be reversed.

You can use the Window > New Window menu command to open additional windows that contain the same statistics. Each of these views can be sorted by a different column. So you can open two Statistics Views, use the Window > Tile command to display one above the other, and then sort one of them for received and the other for sent data.

 If you want to use the data in some other application, you can copy the content of the table as tab separated value list to the clipboard. Therefore click the copy button , use the Edit > Copy menu command, or press Ctrl+C or Ctrl+Insert on the keyboard. Most spreadsheet applications (e.g. Microsoft Excel) will correctly insert this format into a table when you paste it.


 You can at any time click the Empty Buffer button  or use the Collect > Empty Buffer menu command to reset the statistics view and delete all data rows.


 Click the Stop button , use the Collect > Stop menu command, or press Ctrl+F8 on the keyboard to freeze the current statistics display.




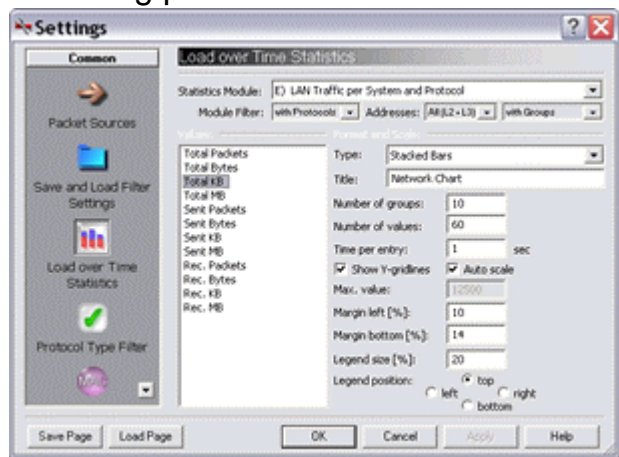
2.3 Load over Time Statistics

(PRO VERSION)



 The Network Load over Time Statistics display the network load per address, network card, protocol, connection, or a combination of these over a configurable period of time. You choose between different chart types to display the data (see Load over Time Charts for more details). The resulting charts can be saved to disk or copied to the clipboard.

To create a new Load over Time Statistics View, click the New Load over Time Statistics button  in the toolbar, use the File > New Load over Time Statistics menu command, or press Ctrl+H on the keyboard. This will open the Settings Dialog for the Load over Time Statistics.

 Open the Load over Time Statistics Settings page of the Settings dialog. As for the standard statistics you can use the other pages in the dialog to configure filters that will restrict the packets that are evaluated for the statistics display. This works in the same way as the capture filter for collecting packets and is described in detail later on.

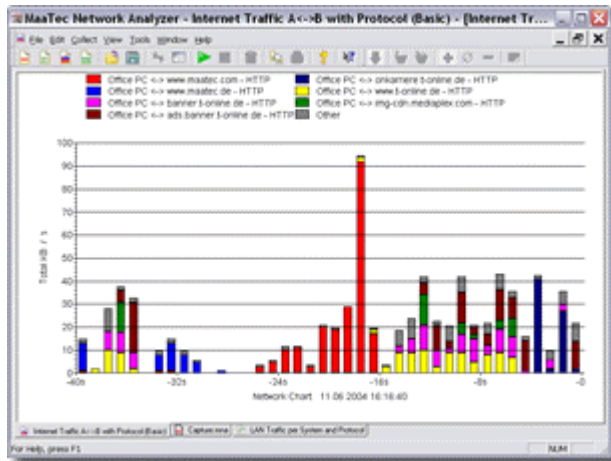



You can choose between different statistics modules to analyze different aspects of the network traffic. A detailed description of the different modules can be found on the Statistics Modules page. Click the Statistics Module combo box and select the 'Internet Traffic A<->B with Protocol (Basic)' in group F) (if you switched off the Easy Statistics Mode, this module is called 'L3 Addr between L3 Addr Higher Protocol Statistics'). Now select 'Total KB' in the values list on the left, select the Stacked Bars chart type, set the number of values to 40 or 50, and the time per entry to 1 second. Then click OK to create a new Load over Time Statistics View.


 If the statistics collection did not start automatically (see Auto-Start Collection option in the Tools Menu), you can start it now by clicking the Start button  in the toolbar, or you use the Collect > Start menu command, or press F8 on the keyboard. If there is any traffic on your network, you should see some bars moving to the left that display the

MaaTec Network Analyzer


connections (with the used protocols) that currently cause the most network traffic.

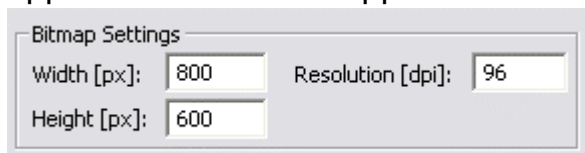


Click the Stop button , use the Collect > Stop menu command, or press Ctrl+F8 on the keyboard to freeze the current statistics display. Though you needn't stop the statistics to save or copy the chart.

You can copy the chart as enhanced metafile to the clipboard. Therefore click the copy button , use the Edit > Copy menu command, or press Ctrl+C or Ctrl+Insert on the keyboard.

Note: While many applications can import enhanced metafiles, you will often not get the same formatting as on the screen. Sometimes it can help to change the width or height of the chart after pasting it into an application (especially if only some legend labels do overlap). If this does not help, you may need to save the chart as bitmap file (see below) and then import this file into the application.












To save the chart to disk, click the Save button , use the File > Save or Save As menu command, or press Ctrl+S on the keyboard. Under file type you can choose between four different bitmap formats and the enhanced metafile vector format. The recommended format is PNG 8 bit, as this will create the smallest files. You should use the BMP format only if your target application does not support the PNG format (which should rarely happen).



If you selected a bitmap format, you can configure the size (in pixels) and the resolution (in dpi) of the bitmap with the controls at the bottom of the dialog. Please note that greater values for the resolution will increase the (pixel) size of the fonts. This may lead to overlapping text if the bitmap size is too small.



2.4 Collecting Packets







-  To collect packets from the network, you need to create a new MTNA document first. You can click the New Packet List button  in the standard toolbar, use the File > New Packet List menu command, or press Ctrl+N on the keyboard to open the settings dialog for the capture filter. The settings dialog allows to change the buffer size for storing collected packets, to choose the network interface cards from which data is collected, to select the columns that shall be displayed in the list, and to configure some filters to reduce the number of packets that will be stored in the document. This time, just click the dialog's OK button.
-  Now you are ready to collect some network data into the new document: If the Auto-Start Collection option in the Tools menu is enabled, the data collection will already run. Otherwise click the Start collect button  in the toolbar, use the Collect > Start menu command, or press F8 on the keyboard. Depending on the network traffic on your computer, you may need to wait a moment to see some packets coming in.
-  As data collection is running, the packet list view will continuously display some information about the collected packets. New packets are added to the end of the list and the view will scroll if needed. You may want to stop the view from scrolling to take a closer look at some packets. To do this, click the Auto Scrolling button  or use the View > Auto Scrolling menu command. Click the button again to reactivate the automatic scrolling.
-  To stop collecting packets, click the Stop collect button , use the Collect > Stop menu command, or press Ctrl+F8 on the keyboard.
-  After you stopped collecting packets, it is possible to clear the view and delete all packets by clicking the Empty Buffer button  or via the Collect > Empty Buffer menu command. But do not do this now if you want to continue with the next quickstart topic.
-  You can also collect packet data directly into disk files. This background capturing can be started manually or via an integrated scheduler. See Scheduled Packet Capturing for more details.

2.5 Analyzing Data





To take a closer look at the navigation and decode features, you should first collect some packets or open a saved network data file. Now the packet list view displays some basic information about the network

packets. You can see the capture time, the raw packet length, the source and destination addresses of the network layers 2 and 3, and the protocol or type of the packet.

-  To get a more detailed description of a packet, click inside the packet list.
-  This will display a clear text description of the packet content in the decode view (on the left below the packet list) and the corresponding hexadecimal values of the decoded data in the hex view (right of the decode view). You can resize these views by dragging the separators between them.
-  The detail level of the displayed data in the decode view can be adjusted. To see the complete packet content with all details, click the All Details button  or use the View > Detail > All menu command. To get only common details, click the Common Details button , to see only the most important information, use the Minimum Details button . As above you can also use the corresponding menu commands in the View > Detail submenu.

The decode and hex view are synchronized. So if you scroll one of them, the other view will also scroll. Thus the hex view always displays the hexadecimal values of the decoded data in the same line as the decode view.

Note: If you encounter some synchronization trouble between decode and hex view, or you have problems to scroll either view all the way down, you will most likely use an old rich edit control. In this case use the full MTNA setup, which will install the needed version of the control.



-  After clicking into the packet list view, you can also navigate through the packets with the keyboard. The left and right cursor keys will change the column. The up and down cursor keys will move the selection in a context sensitive manner. Only in the Time/Length column the selection will change to the next/preceding packet when pressing the cursor down or up key. In the other columns the selection will jump to the next cell with identical content. In the address columns, this will be the next packet with the same source/destination address, and in the type column it will be the next packet of the same protocol (e.g. jump from one HTTP packet to the next ignoring any other packets between these). The Page Up and Page Down keys will move the list one page up or down. The Home and End keys will move the selection to the first and last column, and, if used together with the Ctrl key, they will take you to the first or last packet in the list.
-  You can set bookmarks for selected packets in the list view. For this purpose press Ctrl+F2 on the keyboard or use the Edit > Bookmarks > Toggle Bookmark menu command. Press Ctrl+F2 again to remove the bookmark. You can now use F2 and Shift+F2 on the keyboard or the commands in the Edit > Bookmarks submenu to jump to the next or

previous packet entry that has a bookmark.

Use the Remove all Bookmarks command in the Edit > Bookmarks submenu to remove all previously assigned bookmarks. The bookmarks are saved in the document on disk.



2.6 Printing and Copying





 You can print the contents of the decode or hex view. Click inside one of them and then click the Print button , use the File > Print menu command, or press Ctrl+P on the keyboard.



Alternatively you can get a print preview via the menu command File > Print Preview and then print from inside the preview by clicking the Print button at the top of the preview window.


 If you are not using a color printer or want to get a black and white printout, click the Toggle B/W output button  before printing or use the View > B/W output menu command. This will toggle the views between color and black and white representation.


 To use the decode, hex, or packet list view content in other applications, you can copy it to the clipboard. Select the text with mouse or keyboard and click the copy button , use the Edit > Copy menu command, or press Ctrl+C or Ctrl+Insert on the keyboard. Now you can paste the formatted text in any other application.

2.7 Packet Filtering




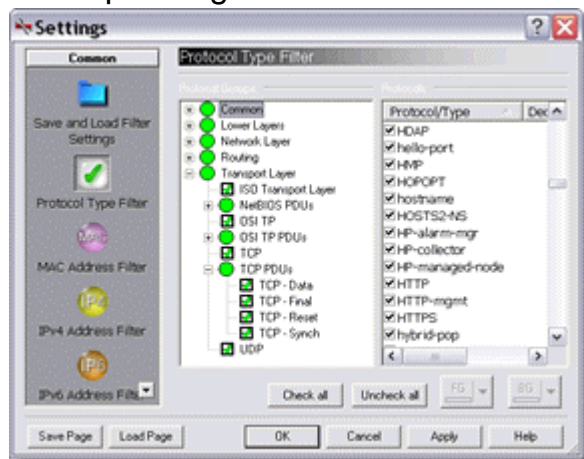
The Network Analyzer offers two types of packet filters. One capture filter per document and one view filter per view. Packets not passing the capture filter will be lost while the view filter will only hide but not remove these packets from the storage. You can look up an overview of the data flow through the application in the reference section.

 As the Settings dialog for both types of filters is almost the same, we'll take only a look at the view filter here. So open a data file or collect some packets first. If you just collected packets, you should stop collecting now. Otherwise the view filter will only be applied to new packets coming in but


not to already visible ones. Though if you stop collecting later, all packets will be filtered then. Now click the View Filter button , use the View > View Filter menu command, or press F10 on the keyboard.

Note: Unlike the view filter, the capture filter is only available for newly created documents as you cannot collect packets into documents loaded from disk. Use the Collect > Capture Settings menu command to open the Settings dialog for the capture filter.

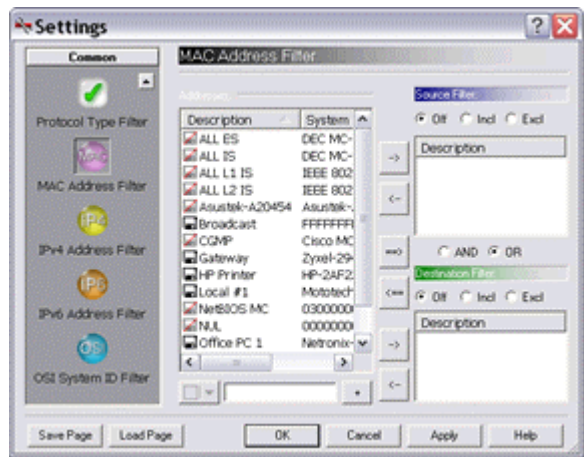
- ✔ Go to the Protocol Type Filter page in the Settings dialog by clicking the corresponding button  on the left.







Now move the Settings dialog until you can see the Type column of the packet list view together with the dialog (the Settings dialog can be resized). Scroll the right (Protocols) column of the dialog to a protocol which is present in the packet list. Alternatively you can click into the protocol list and type the first letters of a protocol name on the keyboard (e.g. h-t for HTTP). Uncheck the protocol entry in the list and click the Apply button. The corresponding packets in the packet list view will disappear. You can try this with other protocols, too. If you have finished, click the Check all button to reset the filter to its initial state and click Apply. With the customizable Protocol Groups tree on the left you can even enable or disable multiple protocols at once. See Protocol Filter Settings for more details.

- ✔ Now open the MAC Address Filter page by clicking the pink button  on the left.

Note: If not all entries in the dialog's page list are visible, you can scroll it by clicking the little arrow buttons or right-click into the list to get a context menu, which allows to switch between large and small icons.





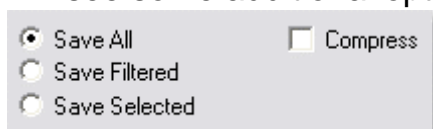
Move the Settings dialog until you see the MAC Src. and MAC Dest. column of the packet list view. In the Addresses list of the filter dialog select an address entry, which is also present in the MAC Src. column. Now click the upper right arrow button  in the dialog. The selected address appears in the Source Filter list, and the Incl option becomes highlighted (if Off was selected before). Click the Excl option instead and close the dialog with the OK button. All packets with the corresponding source address will disappear from the packet list. Take a look at the Address Filter help to learn more about the many ways to add and remove addresses to/from these filters and how to rename or color the address entries for better recognition in the packet list view.

 To remove the view filter click the Remove View Filter button , use the View > Remove View Filter menu command, or press Ctrl+F10 on the keyboard. All packets will reappear. If you open the view filter dialog again, you will be taken to the same page that was open the last time. Also the address filter settings are initialized to the same values. So you can reapply the previous filter just by clicking OK. To reset the filter settings, go to the Save and Load Filter Settings Page  and click Reset All.

2.8 Saving and Loading Data



 To save collected packets to disk, click the Save button , use the File > Save menu command, or press Ctrl+S on the keyboard. This will open the Windows standard dialog for saving files. Near the bottom of the dialog you will see some additional options:







- Save All: This is the default. All packets in the document will be saved in the file.

- **Save Filtered:** This option is only available if you applied a view filter to the current view. It will save all packets which are visible in the list view.
- **Save Selected:** This will save only the currently selected packets.
- **Compress:** The file will be compressed when saved, thus it will use less space on the disk. With external file compression tools you will mostly get higher compression rates, but with the internal compression you can load files without uncompressing them before.

Note: The compress option is only available for data that was collected into the standard packet list. If you load uncompressed data from disk (e.g. after using the scheduled collector that writes data directly to disk), the program uses a different data management approach that can display files that are larger than the available memory, but that is not compatible with data compression.

If you save a file that was already saved to disk, you will not see the standard dialog, but only a small one that offers the above options. To save a file under a new name, use the File > Save As menu command.

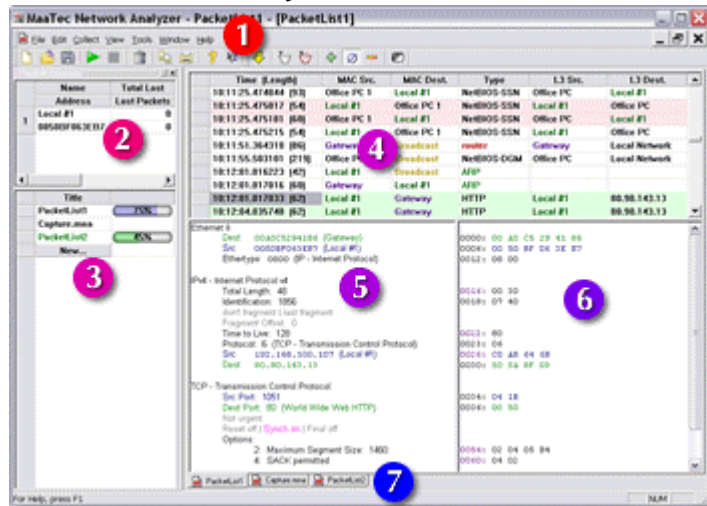
 You load a previously saved file by clicking the Open button , by using the File > Open menu command, or by pressing Ctrl+O on the keyboard. This will show the standard file open dialog where you can choose the file to load. The application will detect itself whether the file was compressed or not.

 To close a view, you can use the standard close button  in the upper right corner of the view window or press Ctrl+F4 on the keyboard. If this was the only view of the corresponding document, the document will be closed, too. If you opened multiple views for a document (e.g. via the Window > New Window command), you can close them all at a time by using the File > Close menu command.



2.9 Main Window Overview

The Network Analyzer Main Window:






- 1 The menu and toolbars of the Network Analyzer. These can be dragged with the mouse. You can attach menus and toolbars to any side of the window, or you can let them float in their own window. New toolbars may be added and their look can be changed in the Customize Toolbars page of the Customize dialog. This dialog can be opened with the Tools > Customize menu command, or you can right-click in the menu or toolbar area and choose Customize in the context menu. The context menu, as well as the View menu, allow to toggle the visibility of the toolbars. The commands offered by menus and toolbars can be modified on the Customize Commands page of the Customize dialog. Here you can also add additional menus.

- 2 This is the Packet Source View. Here you can see the network cards of your system with some additional information.

Note: If the packet source list is empty, you won't be able to collect any network data. This will most commonly happen because either your network cards are disabled or you are not logged on with administrative credentials.

- 3 The Packet Sink View lists all open documents in the application. The right column displays the percentage of the document's packet store that is already filled. Green colored bars and label text indicate that currently data is collected from the network, otherwise the bar is colored blue. If no bar is displayed, the document was loaded from disk.
- 4 The Packet List View displays some basic information about collected network packets including their capture time, the raw packet length, source and destination addresses of the network layers 2 and 3, and the protocol

or type of the packet (you can change the visible columns on the Packet List Columns page of the Settings dialog). Clicking into the list or moving between packets with the cursor keys will show more detailed information about the selected packet in the decode and hex view below the list. You can also right-click an address and use the Properties command in its context menu to open the Edit Address Information Dialog.

- 5 The Decode View displays detailed information in clear text about packets selected in the packet list view. You can change the detail level with these toolbar buttons:    (see Analyzing Data for more information).
- 6 The Hex View displays the raw data values (in hexadecimal format) corresponding to the information on the same line in the decode view. The vertical scrolling of both views is synchronized for this purpose. At the beginning of each line the position of the data in the packet is shown (zero-based decimal). If preceding data is omitted due to the detail settings, the position text will be colored dark pink.
- 7 Clicking the view tabs allows to change the active view in a straightforward manner. You can also use the Window menu for this purpose or press Ctrl+Tab or Ctrl+Shift+Tab on the keyboard. To change the look of the tabs or hide them at all, use the Customize Tabbed MDI page of the Customize dialog.

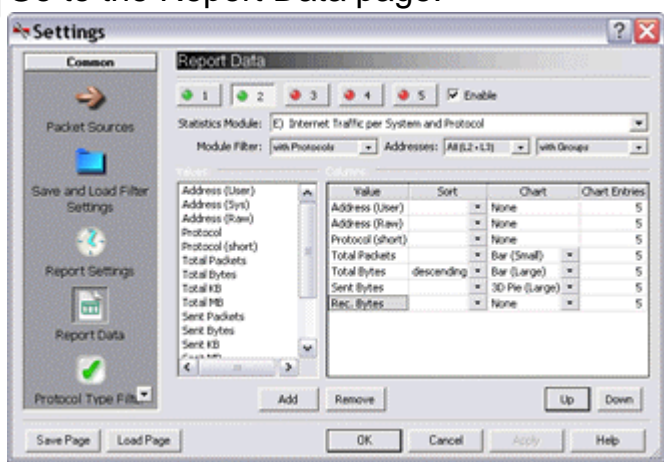
3 Advanced Features

3.1 Generating Reports



(PRO VERSION)

- The MaaTec Network Analyzer can generate network traffic reports. You can customize the report schedule, contents, target directory, and the format of the reports. To start a new report generator, click the New Report button , open the File menu and choose the New Report command or press Ctrl+R on the keyboard. This will open the Settings dialog for reports.
- To get to know the different report options, go to the Save and Load Filter Settings page of the Settings dialog and click the Import button. In the file dialog navigate to the MTNA installation directory and open the ReportDemo.mnset file. This file contains some report settings that will demonstrate many of the report features of the Network Analyzer.
- Now open the Report Settings page. You can change the schedule and file properties for reports here. First choose a directory, where the reports shall be stored. For testing you should set the report frequency and duration to 'every 1 minute for 1 minute'. Otherwise you may need to wait awhile before a report is generated. Check the HTML format box and enable all detail options.
- Go to the Report Data page.



On top of the page you find a row of buttons. Each of these buttons represents a data table that can be included in the generated report. If a table is included in a report, it is marked with a green LED on the button. To edit the properties of a data table, click the corresponding button. This will fill the dialog elements with the currently configured content of this table. To include a table in a report, you need to check the Enable box to the right of the button. To exclude a table, uncheck the box. This will

turn the button LED red. As a report needs to contain at least one data table, the first table will always be enabled.

Below the table buttons you can choose a statistics module that shall be used for the current table (see also Network Statistics). The values and column lists allow to select specific columns (and their units) that shall be included in the final table. You can specify a column here that shall be used for sorting and you can select different charts that will be added below the data table in the report.

If you imported the ReportDemo settings file, click some of the table buttons and take a look at the different settings. Then click the OK button and continue with the next but one paragraph.

If you want to configure the report settings yourself click the table 1 button. Then select the 'LAN Traffic per System' module (or 'L2 Address Statistics' if you switched off the Easy Statistics Mode) in group B). The list on the left now contains all available values (columns) for this module, the column list on the right contains the values that will be actually contained in the report. To add values to the report, select one or more in the Values list and click the Add button or double-click any value entry. To remove values from the report, select them in the columns list and click the remove button. Now add 'Address (User)', 'Address (Raw)', 'Total Packets', and 'Total Bytes' to the columns list. Click the small arrow button in the sort column of 'Total Bytes' and select 'descending'. This means that the report will contain the MAC addresses of all systems that caused any traffic on the network while the data for the report was collected. The list will be sorted according to the number of bytes these systems have sent and received and the system that caused the most traffic will be displayed on top of the list.

After clicking OK in the Settings dialog, the Report View will open and display information about scheduled, running, and failed reports. You can change the above settings later. Therefore open the Settings dialog again via the Collect > Capture Settings menu command. Changes to the schedule will take effect when the next report is scheduled, changes to the data content will be used by the next report that is started.

Note: If you get the message that the report file could not be opened, you have probably used characters in the report file prefix that are not valid for filenames, or you don't have write permission for the target directory. You need to close the report view and create a new one, because currently a restart of a failed report generator is not possible.

Wait until the first report has been created (or close the report view after a scheduled report was started) and open it with your browser. The report will contain as many data tables as you enabled on the Report Data page. Each table may be followed by one or more charts.

If you generated a text report, open it with any text editor. The header and

time information can be switched off on the Report Settings page of the Settings dialog; thus it may be easier to parse the report data with other applications. The collected data is added to the text report as a tab-separated list. This may look a bit confusing in the text editor. But you can copy the data into or open this file with your favorite spreadsheet editor as well. This will in most cases format the data in a more convenient way. Alternatively you may increase the tab width of your editor.

3.2 Advanced Report Topics

(PRO VERSION)



Command line options

You can use command line options to start the creation of network reports with the MTNA application. First you need to create a report settings file. Use the Report Settings and Report Data pages of the MTNA Settings Dialog to configure a report (you can also add protocol and address filters if needed). Then go to the Save and Load Filter Settings page of the Settings Dialog, click the Export button, and save the settings in a file. Now you can use this settings file to start the report generation on start-up of the MTNA application.

Therefore you need to add the `-r` (report) option and the settings file path to the start command for the MTNA application (e.g.: `MTNA -r "C:\mntna_data\MyReport.mnset"`). This will start the Network Analyzer, open a new report generator, load the settings, and schedule a new report (according to the schedule settings in the given file).

Additionally you can add the `-o` (one-time run) option to the command line (e.g.: `MTNA -o -r "C:\mntna_data\MyReport.mnset"`). This will start MTNA and load the settings as above. But the report generation is started immediately (with a 5 second delay to allow the application to initialize itself). Thus all schedule settings you made are ignored except for the report duration. After the time that was set for the report duration has elapsed, the report is saved to disk and the application closes itself.

Note: Make sure not to start more than one instance of the Network Analyzer at once when using the `-o` option. Usually starting MTNA multiple times would switch you to the running instance, but running in one-time mode will close the application when the first report is finished, so you may get unexpected results in this case.

Using the Windows Task Scheduler

The command line options allow to use the Windows Task Scheduler to run MTNA reports. The Task Scheduler is automatically installed on Windows 2000, 2003, and XP systems. For other operating system versions you may

need to install it with the Microsoft Internet or Platform SDK (or use the AT command line tool in Windows NT 4 and higher). Open the Task Scheduler via the Start menu: Programs > Accessories > System Tools > Scheduled Tasks. Or double-click the Scheduled Tasks entry in the Control Panel window. Double-click the Add Scheduled Task entry in the task list and follow the instructions. Browse for the MTNA application (MTNA.exe) and choose it as application to run. Configure the desired start frequency and time. Use an account with administrative credentials and a valid password for running the task. On the last page check the 'Open advanced properties for this task when I click Finish' option and click Finish. Now add the above options and the settings file path to the start command. See the Task Scheduler help for its other options.

You can use the Task Scheduler for different purposes:

- Use the -r option without -o to start the MTNA application on system start-up and schedule the report generation via the report settings file.
- Use -r and -o to start the application with the Task Scheduler on a regularly basis and set the report duration in the report settings file. This way the Network Analyzer will close itself when the report is finished.
- Start the application with -r and -o options as above, but set the duration in the settings file to a rather high value (e.g. 24 hours). Now use the Advanced tab of the Task Scheduler to set the desired report duration. This way the Task Scheduler will close the MTNA application after the specified time. The report will be created with the correct ending time.

Tips for running long-term reports

When creating one or multiple reports over a long period of time, it is possible that the address database becomes too large so that the overall system performance decreases. To avoid this, you can either use the Windows Task Scheduler to periodically restart the Network Analyzer (see above). This will remove all non-persistent address entries from the database. Or you switch off the auto-update of the address database in the Tools menu. This will prevent the network analyzer from adding new addresses to the database. Any data for addresses that are not found in the address database will then be added to a default address group, e.g. 'LAN' for unknown MAC addresses or 'Internet (v4)' for unknown IP addresses. These names are also used in the reports to display the sum of all traffic from and to addresses that were not present in the database. This is especially useful if you aren't interested in the contacted remote addresses but want only to log the overall traffic of a small number of computer systems. You can further reduce the size of reports by combining this with address group statistics (see Address Groups).

Modifying the style of HTML reports

When a report in HTML or XHTML format is created, the application will check the report destination directory for the files `mtna.css`, `ascend.png`, and `descend.png`. If the files are not found, they will be copied from the MTNA installation directory. Thus you can edit these files in either directory. Modify the files in the installation directory if you want to change the style for all new reports (you will need to copy the files to existing report directories, as MTNA won't overwrite existing style files). Or change the files in any report destination directory to change only the style of the reports in this directory. The png files contain the arrow graphics for marking the sorted columns. Use any graphics editor that can load and save png files to change these images. The `mtna.css` file is the style sheet for all reports in the same directory. Use any text editor or style sheet editor (e.g. the free TopStyle Lite from Bradbury Software) to modify the report styles.

Following table lists the most important styles in the file and what they are used for:

H1	This style is used for the report statistics module titles (the titles above each table). You can change the font-family to "Times New Roman", Times, serif; or the font-size here.
TD.title_l	Style for the left part of the report title (the title that is entered on the Report Settings page).
TD.title_r	Style for the right part of the report title where the computer name is displayed.
TABLE.report	Style for the report tables. You may change the font-size for the table here. You should use one of the size names here (large, medium, small) and not a fixed point size, as then the user may not be able to change the overall font size in its browser.
TR.heading	This style is used to set the background color and font-weight for table and chart titles.
TR.data1	Style for odd data rows in data tables.
TR.data2	Style for even data rows in data tables. Set the background-color property here to get a different background color for every second row in a table.
TD.barfull	Style for filled bars in the HTML horizontal bar charts. You can change the bar and border colors here.
TR.barsep	This style can be modified to set the distance between bars in horizontal HTML bar charts.



3.3 Coloring the List View

You can apply colors to the text and background of different elements in the packet list view. This is especially useful for better distinction of addresses and protocols. You can change the colors in the following areas:

15:49:54.866533 [187]	Local #1	NetBIOS MC	NetBIOS			
15:50:09.375810 [187]	Local #2	NetBIOS MC	NetBIOS			
15:50:17.796530 [86]	Gateway	Broadcast	RIP	Gateway	Local Network	
15:50:22.394602 [250]	Local #1	Broadcast	NetBIOS-DGM	Local #1	Local Network	
15:50:25.583339 [42]	Local #1	Broadcast	ARP			
15:50:25.584168 [60]	Gateway	Local #1	ARP			
15:50:25.584210 [62]	Local #1	Gateway	HTTP	Local #1	80.190.43.13	
15:50:25.655440 [62]	Gateway	Local #1	HTTP	80.190.43.13	Local #1	



- 1 The color of the Time/Length information is used to distinguish packets that were collected from different network interface cards. You can change this color in the packet source view.
- 2 You can apply colors to any address description in the address database. Either right-click an address name in the packet list and choose Properties in the context-menu to open an edit dialog, or change the address colors on the address filter pages of the Settings dialog.
- 3 The text color of protocol names is set on the protocol filter page of the Settings dialog.
- 4 The background color of the rows in the packet list view depends on the protocols used in the corresponding packet. Consequently the background color is also set on the protocol filter page of the Settings dialog. But in contrast to the protocol foreground color, the background color may be deduced from the packet's lower layer protocols. If, for example, no background color was set for the HTTP protocol, the application will look whether some color was applied to one of the packet's lower layer protocols (TCP, IP, etc.). The first background color found, searching from upper to lower layer protocols, will be used.


Note: The default configuration assigns background colors to TCP Synch (green), TCP Reset (yellow), and TCP Final (red) packets.



3.4 Scheduled Packet Capturing

(PRO VERSION)


 To start the scheduled or manual direct to disk packet capturing, click the New Packet Collector button , use the File > New Scheduled Collector command, or press Ctrl+D on the keyboard. This will open the Settings dialog for scheduled packet capturing.

 Now open the Scheduled Packet Capture Settings page. You can toggle between manual and scheduled start of the packet capturing, set the target directory and file prefix for the created data files, and you can configure the schedule for capturing data.

You should first set the target directory to a meaningful path here, as the program may not have write access to the directory that was set as default. After clicking OK in the Settings dialog, the Scheduled Capture View will open and display information about scheduled, running, and failed packet collectors. You can change the above settings later. Therefore open the Settings dialog again via the Collect > Capture Settings menu command. Changes to the schedule will take effect when the next collection is added to the schedule table, changes to the data content will be used by the next collection that is started.

Note: If you get a message that the data file could not be opened, you have probably used characters in the file prefix that are not valid for filenames, or you don't have write permission for the target directory. You need to close the scheduled capture view and create a new one, because currently a restart of a failed data collection is not possible.

Wait until the first file has been created (or close the view after a scheduled collection was started) and open it with the Network Analyzer. Now you can view the collected data in the Packet List View.

 You can also use command line options to start collecting packets when the Network Analyzer is started. First you need to create a scheduled capture settings file. Therefore start a new scheduled collector as described above. When you have made your settings, do not click the OK button of the Settings dialog. Instead of closing the dialog, go to the Save and Load Filter Settings page, click the Export button, and save the settings in a file. Now you can use the option -c (collector) and the settings filename as command line options for the Network Analyzer program, e.g. `MTNA -c "C:\mntna_data\MyCollector.mnset"`. This will start the configured collector on start-up of the Network Analyzer.

Please see Advanced Report Topics for more tips on using the command line.

3.5 Customizing the Application



You can customize many parts of the Network Analyzer user interface. To change or add keyboard shortcuts, use the Shortkeys page of the Customize dialog. You can also customize the toolbar buttons and menus there or even add additional toolbars. And you can change the look of the window tabs at the bottom of the main window in the dialog. To open the

Customize dialog, use the Tools > Customize menu command or right-click in the menu or toolbars area to open a context menu with a Customize command.

You can change the address names and colors that are displayed in the packet list view. See [Coloring the List View](#) for more information.

You can modify configuration files used by the Network Analyzer to add or modify NIC vendor names and TCP ports and their descriptions. This is described in [Modifying the configuration files](#).

If you use some capture or view filter settings frequently, you can add them to the Quick Load list on the Save and Load Filter Settings page of the Settings dialog for filters. And you can modify the Protocol Groups tree on the Protocol Type Filter page of the Settings dialog by dragging and dropping protocol entries from the protocols list on the same page.

Most of the settings are automatically saved in the application's settings file, but you can also export these settings to disk to share them with other instances of the Network Analyzer on other systems (see [Saving and Loading your Settings](#)).

3.6 Modifying the configuration files



The MaaTec Network Analyzer uses a number of configuration files for decoding and displaying network packets. The files should have been installed to the same directory as the Network Analyzer application. If you change these files, you need to restart the application. Currently the following files are used:

Vendor.Codes

This file contains vendor or manufacturer codes that are used to create better readable names for MAC addresses. You can add codes to the list in the following format: start with 6 hexadecimal digits for the vendor code followed by a short description. A complete list of up to date vendor codes can be found at <http://standards.ieee.org/regauth/oui/oui.txt>.

tcp.ports

This file contains TCP and UDP port numbers and corresponding protocol names and descriptions. These are used by the TCP and UDP decoders and filters. Every line should start with a port number in either decimal or hexadecimal (use 0x as prefix) format. Then follows a protocol name that must not contain any spaces and a short description. Any line that does not start with a digit is supposed to be a comment. An up to date list of assigned TCP and UDP port numbers can be found at <http://www.iana.org/assignments/port-numbers>.

udp.ports

This file uses the same format as the tcp.ports file. It contains only port numbers that are not assigned to the same protocol as in the tcp.ports file.

ipx.sockets

This file is used to map IPX socket values to their corresponding protocol names and descriptions. It has the same format as the tcp.ports file.

Note: If you frequently use vendor codes or common port numbers that are missing in the lists, you may send an email to support@MaaTec.com, so that these numbers can be added to the lists.

3.7 Saving and Loading your Settings



Most of your current settings are saved in the user settings file when the Network Analyzer application is closed. But you may probably want to reuse some of your filter settings at a later time, or you want to share filter settings or network address names with other users. In this case you can save or export your settings in many ways.

If you want to reuse specific filter settings, you should add them to the Quick Load list on the Save and Load Filter Settings page of the filter Settings dialog. You can also export your filter settings to disk or import settings from disk on that page.

If you just want to save the settings of one of the dialog pages, you can use the Save Page and Load Page buttons in the lower left corner of the dialog window. Notice that you can only load settings on the same page that was used for saving.

Address descriptions and colors are not saved together with the filter settings. To export or import the address database, use the corresponding menu commands in the File menu. You need to mark address entries in the database as persistent to export them to a file. This is done automatically when you change the description or color of the address. Alternatively you can toggle the persistence state of the address entries on the Address Filter page of the Settings dialog.

3.8 System Performance and Packet Loss



Losing packets means that the Network Analyzer is not able to collect as many network packets as are received by the system. If the network driver cache is full, the driver will reject incoming packets and increase a lost packets counter.

This value is saved in the next packet that is not rejected. You can see the number of packets that were lost between a packet and its predecessor in the Time/Length column of the packet list view. The packet source view displays the number of packets that were lost on each network card since the application started (Total Lost) and since the last collection started that used the network card (Lost Packets).

Packet Sources		
	Name	Total Lost
	Address	Lost Packets
1	Local #1	90
	0050BF063EB7	35

Time (Length)		
18:50:34.835888	(77)	Lost: 1
18:50:34.916531	(62)	Lost: 2
18:50:34.992668	(54)	Lost: 2
18:50:35.076790	(94)	Lost: 2

If any filters are active (capture and/or view filters), the number of lost packets will be summed up and added to the next packet that is displayed in the packet list. That way you will always know where you can trust your data and where you may have lost some information.







Note: The number of lost packets is saved together with the packet contents on disk. But if you save only selected or filtered packets, some of this information may get lost. So if you lost some packets and need to know where these packets were lost, you should always save all packets to disk (see Saving and Loading Data).

If the Network Analyzer loses packets, this can have multiple reasons:

1. Too many other applications are running on your computer. Your CPU load needn't be near 100% in this case. You may already lose packets if another application frequently accesses the system bus. Try to close some other applications in this case or use a different computer for analyzing your network traffic. Especially running an online virus scanner and the Network Analyzer on the same machine may significantly increase the CPU load.
2. Your system is too slow. Try to use a capture filter, but in most cases you need to use a more powerful computer to collect network data.
3. Too many collecting documents are open at once. This will rarely happen as the packet dispatcher and the packet filters of the Network Analyzer are highly optimized. But if you have multiple network interface cards in your system, try to collect data only from one card at a time.
4. Insufficient memory: Each document that collects data from the network needs about its buffer size plus 50% of your system's memory. If there is not enough free memory, Windows will swap parts of the used memory to disk, which will considerably degrade the system performance. In this case, try to close other applications, use less documents at a time, or reduce the buffer size when creating documents.

4 More Help



-  You can get context-sensitive help while using the Network Analyzer. You may always press F1 on the keyboard to get help. Depending on the active window or dialog, this will open the MTNA help file or display a text box near a selected dialog element.
You can also use the Help > Help Topics command to open the MTNA help file, and some dialogs offer a Help button to get context help.
-  Clicking the Help button in the toolbar  will change the shape of the mouse pointer. Now you can click any window element or menu command to get help for the respective item.
-  Some dialogs offer so-called 'What's this?' help. Click the question mark button  in the title bar of the dialog to change the shape of the mouse pointer. Now click any dialog element to open a text box with a short description.
-  If you have more questions regarding the MaaTec Network Analyzer, visit the MTNA web site at www.MaaTec.com/mtna/index.html, or send an email in English or German to support@MaaTec.com.

5 Reference

5.1 Main Window



Menus → File Edit Collect View Tools Window Help

Toolbars → [Icons for file operations, search, and analysis]

Packet Source View

Name	Total Lost
Local #1	0
0050BF063EB7	0

Packet Sink View

Title	Percentage
PacketList1	75%
Capture.mna	45%
PacketList2	45%
New...	

Packet List View

Time (Length)	MAC Src.	MAC Dest.	Type	L3 Src.	L3 Dest.
10:11:25.474844 (93)	Office PC 1	Local #1	NetBIOS-SSN	Office PC	Local #1
10:11:25.475017 (54)	Local #1	Office PC 1	NetBIOS-SSN	Local #1	Office PC
10:11:25.475181 (60)	Office PC 1	Local #1	NetBIOS-SSN	Office PC	Local #1
10:11:25.475215 (54)	Local #1	Office PC 1	NetBIOS-SSN	Local #1	Office PC
10:11:51.364310 (86)	Gateway	Broadcast	router	Gateway	Local Network
10:11:55.503101 (219)	Office PC 1	Broadcast	NetBIOS-DGM	Office PC	Local Network
10:12:01.016223 (42)	Local #1	Broadcast	ARP		
10:12:01.017016 (60)	Gateway	Local #1	ARP		
10:12:01.017033 (62)	Local #1	Gateway	HTTP	Local #1	80.90.143.13
10:12:04.035748 (62)	Local #1	Gateway	HTTP	Local #1	80.90.143.13

Decode View

```

Ethernet II
  Dest: 00A0C5294186 (Gateway)
  Src: 0050BF063EB7 (Local #1)
  Ethertype: 0800 (IP - Internet Protocol)

IPv4 - Internet
  Total Length: 48
  Identification: 1856
  don't fragment | last fragment
  Fragment Offset: 0
  Time to Live: 128
  Protocol: 6 (TCP - Transmission Control Protocol)
  Src: 192.168.100.107 (Local #1)
  Dest: 80.90.143.13

TCP - Transmission Control Protocol
  Src Port: 1051
  Dest Port: 80 (World Wide Web HTTP)
  Not urgent
  Reset off | Synch on | Final off
  Options:
    2: Maximum Segment Size: 1460
    4: SACK permitted
    
```

Hex View

```

0000: 00 A0 C5 29 41 86
0006: 00 50 BF 06 3E B7
0012: 08 00

0016: 00 30
0018: 07 40

0022: 80
0023: 06
0026: C0 A8 64 68
0030: 50 5A 8F 0D

0034: 04 1B
0036: 00 50





0054: 02 04 05 B4
0060: 04 02
    
```

5.1.1 Packet Sources Window



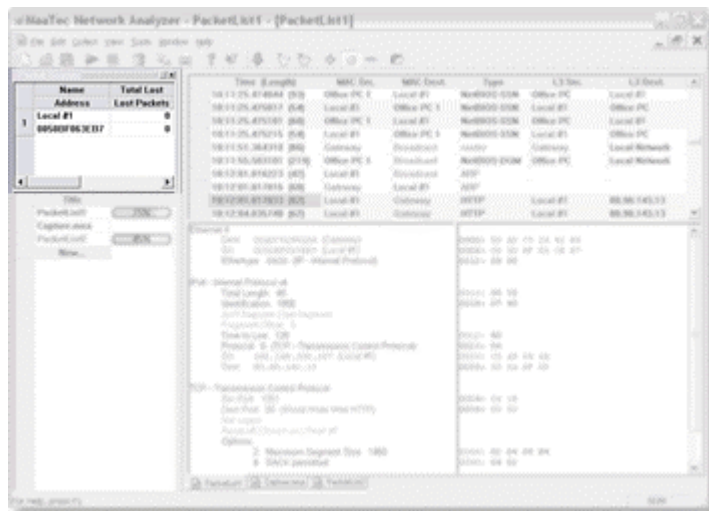
The Packet Sources window contains the Packet Source View and the Packet Sink View. You can click the window title bar and hold the mouse button down to drag the window anywhere you want. The window can float

in its own frame, or you can attach it to any side of the main window.

-  You can toggle the visibility of the Packet Sources window by clicking the
-  Packet Sources toolbar button . If the window is visible, you can also click the small close button  in the upper right corner of the window to hide it. To show the window again, use the View > Packet Sources menu command.



5.1.2 Packet Source View



The Packet Source View is located in the upper area of the Packet Sources Window. It contains five columns with two lines of information for each network interface card that was found on your system.

	Name	Total Lost	Medium	Text Color	Description [Registry]
	Address	Last Packets	Link Speed	Frame Size	Description [Device]
1	Local #1	0	Ethernet	Text Color	Realtek RTL8139[A] PCI-Fast Ethernet-Adapter
	00E07D95B958	0	100 Mbps	1514	Realtek 8139-series PCI NIC
2	Local #2	0	Ethernet	Text Color	Intel[R] PRO/100 VE Network Connection
	00E018A20454	0	10 Mbps	1514	Intel 8255x-based Integrated Fast Ethernet

- 1 The first column contains the names and MAC addresses of the network cards. You can double-click a name or press F2 or Insert on the keyboard while a name is selected to edit it. The names will be used in the packet list view when packets containing this address are displayed.
- 2 The second column displays summary information on how many packets were lost while collecting data from this network interface. The upper line lists the number of packets that were lost since the application started, the lower line contains the number of packets that were lost since you started collecting data with this network card the last time.
- 3 The third column displays the network medium and the detected link speed of the network interface.

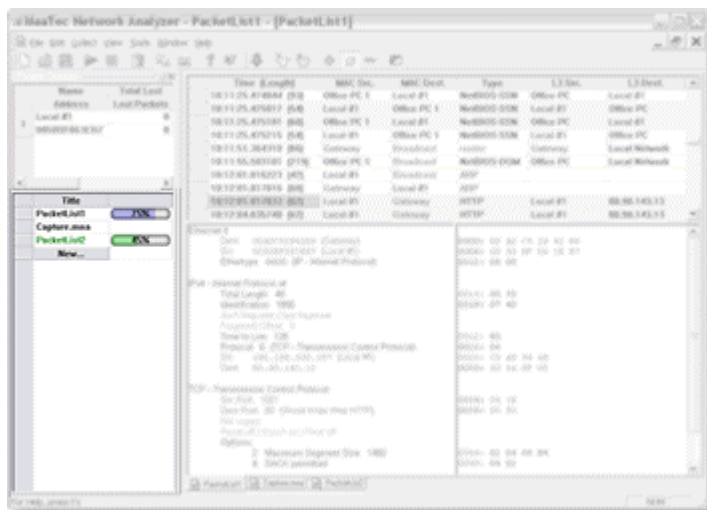
Note: The displayed link speed need not be the maximum speed of your network card. It can be lower if the card was connected to a hub or switch that does not support the link speed of the network card. Also if the card is

not connected at all, it will report a default link speed that may be lower than its maximum speed.

- 4 The fourth column contains a text color selector and the detected maximum frame size of the packets collected by this NIC. The text color is used for the Time/Length information in the packet list view. This allows to distinguish between packets from different sources. You can change the color by clicking the button on the right of the Text Color label.
 - 5 The fifth column displays some NIC details found in the registry and reported by the device driver.
- x** You can hide the packet source and sink window by clicking the small close button **x** in the upper right corner of the window. To show the window again use the View > Packet Sources menu command.



5.1.3 Packet Sink View

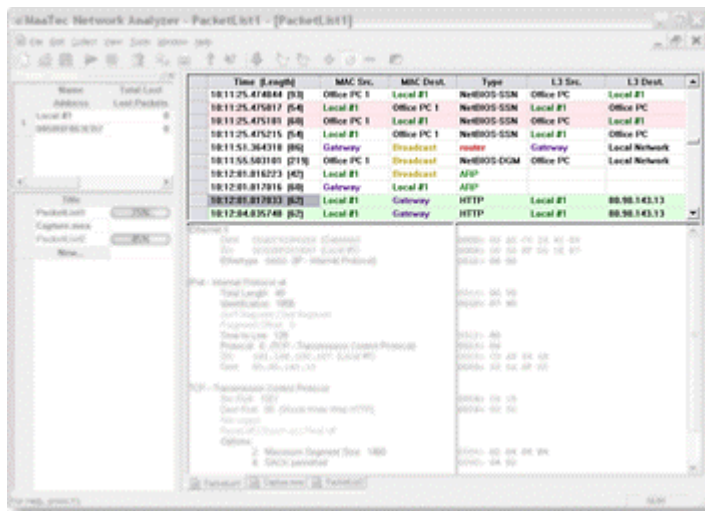


The Packet Sink View is located in the lower area of the Packet Sources Window. It contains a list of all open documents in the Network Analyzer application. If a Packet List document was newly created, the right column of the list will display the percentage of the document's packet store that is already filled. Green colored bars and label text indicate that currently data is collected from the network into this document. If no data collection is running, the bar is colored blue. If the document was loaded from disk, the right column is empty.

The New button in this view allows to create the same new documents as the standard File menu.



5.1.4 Packet List View





The Packet List View displays a list of the packets that are currently stored in the document. By default it contains six columns, but you can change the layout in the Settings dialog on the Packet List Columns Settings page. The default columns will display the following information (see Packet List Columns for more information on these and the other possible column types):



- Time (Length)** The capture time and raw length of the collected packet. The time is displayed as local time of your system in hours, minutes, seconds, and micro-seconds. If some packets were lost before this packet was collected, the number of lost packets is displayed here as well (see also System Performance and Packet Loss).
- MAC Src.** The MAC address of the sender of this packet in the LAN.
- MAC Dest.** The MAC address of the recipient of this packet in the LAN.
- Type** The highest detected protocol of the packet (usually Layer 4 or upper layer protocols).
- L3 Src.** The layer 3 source address of the packet. The type of address depends on the network protocol used for the packet. It can be an IP-address, an IPX-address, or a NSAP address. Not all packets need to have layer 3 addresses.
- L3 Dest.** The layer 3 destination address. It is of the same type as the layer 3 source address.

Note: If you collect packets from different network cards you may experience some irregularities in the time display. This can happen because the application accesses each network interface in a different


thread. These threads now receive one after the other a time slice from the operating system to report their collected packets to the packet dispatcher of the application. Thus the packets that were collected on one NIC during the last 12 ms (time depends on the OS) are stored in one scoop. Then the packets of the next card are stored and so on. Hence the capture time of packets collected from different network cards may slightly overlap.

 You can use a view filter to reduce the number of packets that are contained in the list. Click the View Filter button , use the View > View Filter menu command, or press F10 on the keyboard. This will open the Settings dialog that allows to choose the addresses or protocols of the packets you want to see in the list.

In this dialog you can also change most of the colors that are used in the list view to display the packet information (see Coloring the List View).

 You can remove the view filter to see all packets again. Click the Remove View Filter button , use the View > Remove View Filter menu command, or press Ctrl+F10 on the keyboard.

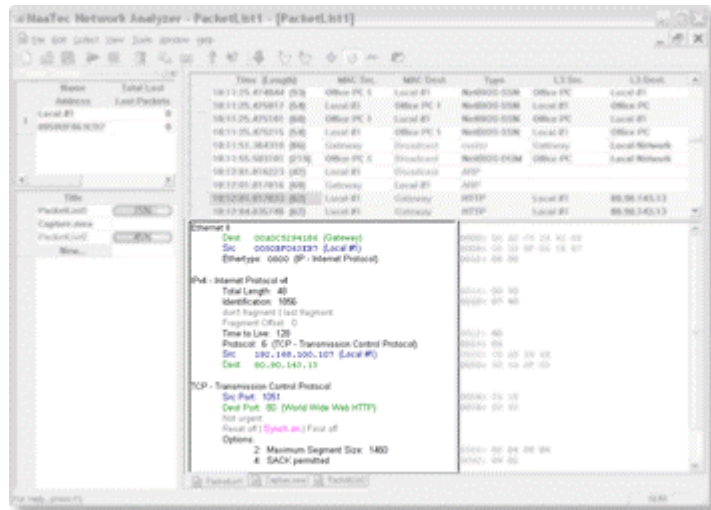
Click inside the list view to display more information about a packet in the Decode View and Hex View below the packet list. Right-click an address and use the Properties command in its context menu to open the Edit Address Information Dialog.

 The packet list view offers also a very convenient way to navigate through the packets with the keyboard. The left and right cursor keys will change the column. The up and down cursor keys will move the selection in a context sensitive manner. Only in the Time/Length column the selection will change to the next/preceding packet when pressing the down or up keys. In the other columns the selection will jump to the next cell with identical content. In the address columns this will be the next packet with the same source/destination address, in the type column it will be the next packet of the same protocol (e.g. jump from one HTTP packet to the next, ignoring any other non-HTTP packets between these).

The Page Up and Page Down keys will move the list one page up or down. The Home and End keys will move the selection to the first and last column, and, if pressed together with the Ctrl key, they will take you to the first or last packet in the list.



5.1.5 Decode View



The Decode View displays detailed information about the packet that was selected in the Packet List View. The corresponding binary data is displayed in hexadecimal format in the Hex View on the right of the decode view. Source addresses and ports are displayed in blue, destination addresses and ports in green.

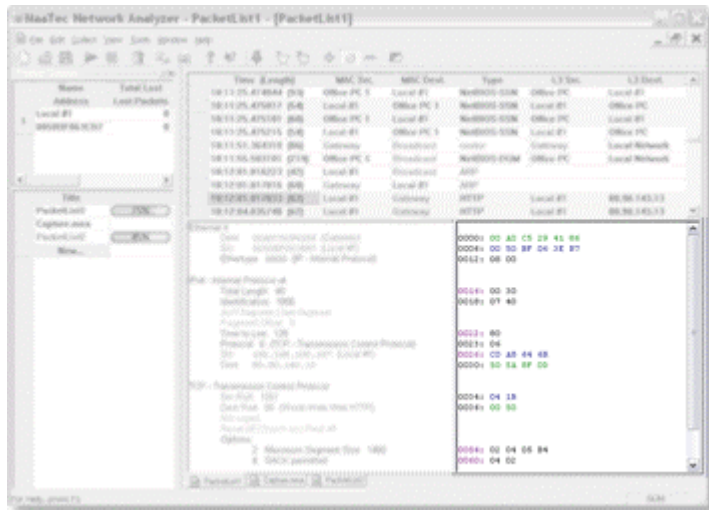
- The detail level of the displayed data in the decode view can be adjusted.
- To see the complete packet content with all details, click the All Details button or use the View > Detail > All menu command. To get only common details, click the Common Details button . To see only the most important information, use the Minimum Details button . As above you can also use the corresponding menu commands in the View > Detail submenu.

If you reduce the detail level, some flag information may only be displayed partially. In this case the text will become gray to indicate that the corresponding value is not visible in the hex view.

- You can toggle between colored text display and black and white text display with the Toggle B/W output button or the View > B/W output menu command.
- To print the contents of the view use the Print button or the File > Print menu command. You can also use the File > Print Preview menu command. See Printing and Copying for more information.



5.1.6 Hex View



The Hex View displays the hexadecimal values of the binary packet data that correspond to the decoded information on the same line of the Decode View.

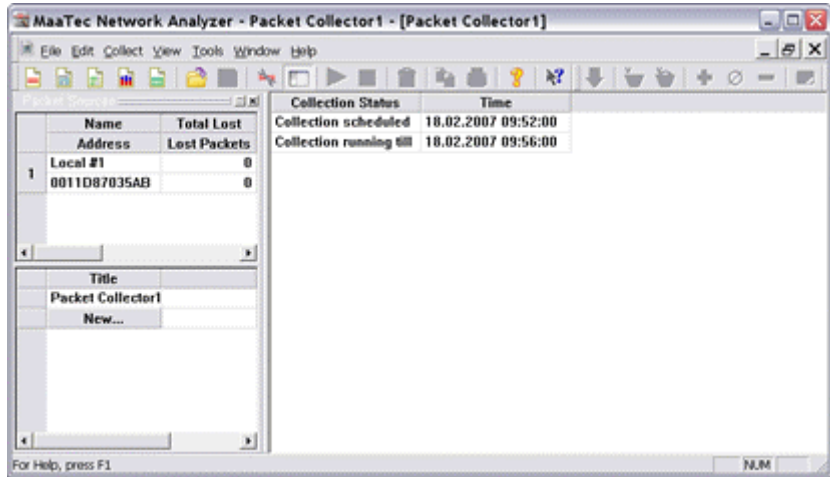
The first number on each line is the zero-based decimal position of the following byte in the packet.

- 🔍 If you reduce the detail level of the displayed data to common 🔍 or minimum 🏠, the position number will be colored dark-pink where data is omitted. As in the decode view, source address bytes are colored blue, and destination address bytes are colored green.
- 🔍 You can toggle between colored text display and black and white text display with the Toggle B/W output button 🔄 or the View > B/W output menu command.
- 🖨️ You can print the contents of the view by clicking the Print button 🖨️ or by using the File > Print menu command. Alternatively you can display a print preview with the File > Print Preview menu command and use the buttons inside the preview window to print the text.



5.1.7 Scheduled Capture View

(PRO VERSION)



The Scheduled Capture View displays information about scheduled and running packet collection tasks. The first line will usually display the time when the next data file will be created. The following line will display running capturing tasks and their respective finishing time. If your capturing times do not overlap, you will not see more than two lines at once. If something went wrong, you will see an error message in one of the lines. In this case try to fix the problem. (You may need to change the prefix for the filename, e.g. due to invalid characters. Or you need to use a different target directory for your data files for which the program has write access. Use therefore the Scheduled Packet Capture Settings page of the Settings dialog.) You will always need to close the failed capture view and start a new scheduled collector.

If this view (or the application) is closed while data is captured, the data file will be created with all packets that have yet been collected.

See Scheduled Packet Capturing for an introduction to the Scheduled Collector.



5.1.8 Statistics View



Address (Host)	Protocol (Host)	Total KBytes	Max. Total KBytes	Sent KBytes	Rec. KBytes
Local #1	HTTP	848	518	2%	55%
www.kiv-vst.com	HTTP	848	458	55%	2%
AMC1700	SMTP - Echo	0	0	0%	0%
AMC1700	NetBIOS-SMB	0	0	0%	0%
Local #1	SMTP - Echo	0	0	0%	0%
Local #1	NetBIOS-SMB	0	0	0%	0%
Gateway	DNS	0	1	0%	0%
Local #1	DNS	0	1	0%	0%
www.maaTec.com	HTTP	0	500	0%	0%

The Statistics View displays the current network traffic that is collected from one or more network cards of your system (specific cards can be selected on the Packet Sources settings page). Read the introduction 'Network Statistics' first if you want to know how to create different Statistics Views.

The traffic is displayed together with addresses, connections, and/or protocols that caused that network traffic. See Statistics Settings and Statistics Modules for more details. You can change the order of the displayed data by sorting any of the data columns: Clicking once on a column heading will sort the values in ascending order for text columns and in descending order for numerical value columns. Clicking again on the heading of a sorted column will change the sort direction. The column that is currently used for sorting is marked with a small arrow that indicates the sort direction.

The traffic data is updated every 0.5 seconds and the average values of the last 2 seconds are displayed.

You can change the statistics settings of the current view in the Settings dialog. This can be opened via the Collect > Capture Filter menu command. You can open another view with the same statistics via the Window > New Window menu command. This new view can be used to display the same data in a different order (e.g. one view sorted for received packets the other sorted for sent packets).

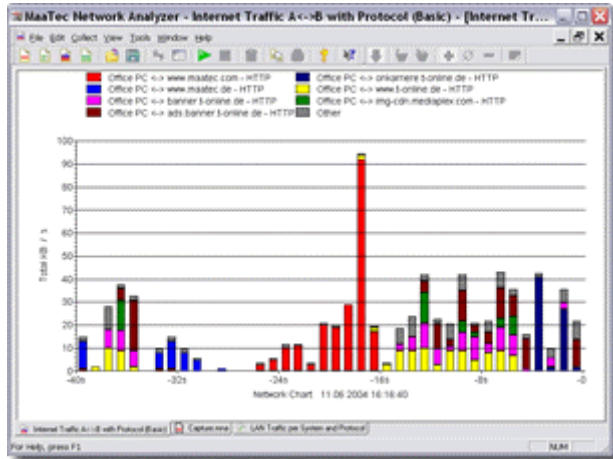
You can freeze the current statistics view with Stop button , by using the Collect > Stop menu command, or by pressing Ctrl+F8. And you can at any time click the Empty Buffer button  or use the Collect > Empty Buffer menu command to reset the statistics view and delete all data rows.

If you right-click an address and use the Properties command in its context menu, the Edit Address Information Dialog will be opened.



5.1.9 Load over Time Statistics View

(PRO VERSION)



The Load over Time Statistics display the network load over a configurable period of time. You can choose between different chart types to obtain information about the traffic that was caused by specific networks, systems, protocols, connections, or some combinations of these.

If this is the first time that you want to use the Load over Time Statistics, you may want to read the introduction in the Quickstart chapter first. You can configure the Statistics Module that shall be used, the chart type, the time settings, and the layout of the chart on the Load over Time Statistics Settings page of the Settings Dialog that is opened when you create a new Load over Time Statistics View.

The maximum number of different data groups that can be displayed in a chart is 10. You will always see the network traffic sources that caused the most total traffic over the configured period of time. One data group is always reserved for 'other' traffic. This group is always displayed as gray bar or line. It contains traffic that was generated by other groups that are currently not the top causers of traffic as well as rounding differences that may arise if not a byte based value type was chosen.

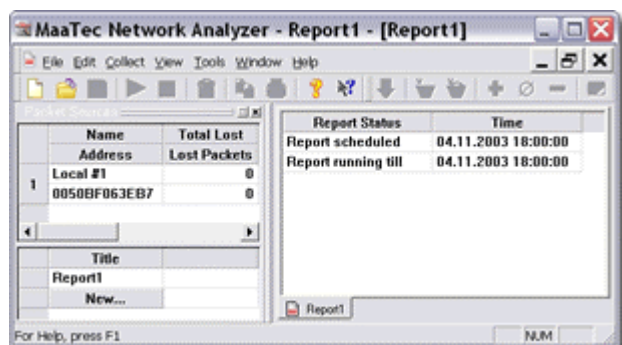
Note: If you use 'Internet..' (or 'L3 Addr...') statistics modules, you may not see the total amount of network traffic in the chart as LAN only packets (e.g. ARP) will not be evaluated by the statistics collector.

You can copy the chart as enhanced metafile to the clipboard or save the chart as bitmap (PNG, BMP) or metafile to disk. The Quickstart introduction describes this in more detail.



5.1.10 Report View

(PRO VERSION)




The Report View displays information about scheduled and running reports. The first line will usually display the time when the next report is started. The following line will display running reports and their respective finishing time. If your reports do not overlap, you will not see more than two lines at once. If something went wrong, you will see an error message in one of the lines. In this case try to fix the problem. (You may need to change the prefix for the filename or the target directory of your reports on the Report Settings page of the Settings dialog.) Always close the failed report view and start a new report generator.

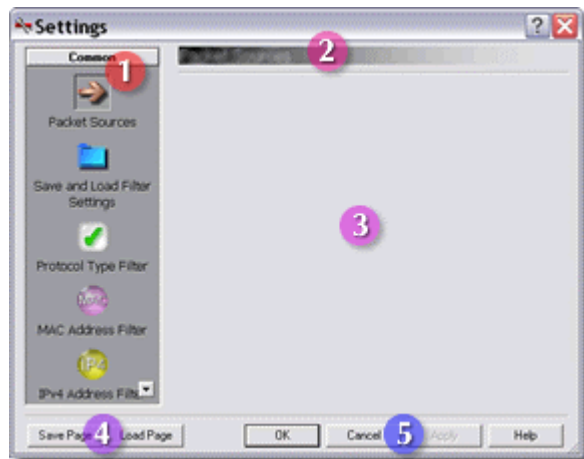
If a report view (or the application) is closed while a report is running, the report will be created with all data that has already been collected for this report and its end time will be set to the time when the view was closed. See Generating Reports for an introduction to report generation with the MaaTec Network Analyzer.

5.2 Dialogs



5.2.1 Settings Dialog

The Settings dialog is used to adjust and manage buffer and filter settings for documents (Capture Filter) and for views (View Filter). It contains therefore a number of configuration pages, which can be selected in the page list on the left. The dialog can be resized. The Collect > Capture Filter and View > View Filter menu commands and the View Filter button  will open this dialog.




- 1 The page list contains entries for all available configuration pages. If not all items are visible in the list, you can either resize the dialog, scroll the list up or down with the small arrow buttons at the top and bottom, or you right-click the list to get a context menu that offers commands to change the size of the icons.

Following pages are available:

- ➔ The Packet Sources page is only available in the Settings dialog for capture filters. It is used to set the buffer size of the document's packet store and the network interface cards, from which packets shall be collected.
- 📁 The Save and Load Filter Settings page is used to save filter settings in the internal settings file (Quick Load list) or on disk and to manage and load these saved settings.
- ✅ The Protocol Filter Settings page is used to configure a protocol filter for the current document or view.
- 🟪 The Address Filter Settings pages are used to configure different address filters for the current document or view.
- 🟪 The Address Group Settings page is used to manage and create new address groups.
- 📊 The Packet List Columns page is used to configure the different packet data columns that shall be displayed in the Packet List View.
- 🌐 The Scheduled Packet Capture Settings page is used to configure the schedule and target directory for the scheduled packet capturing.
- 📊 The Statistics Settings page is used to configure the statistics module that shall be used and the data columns that shall be displayed in the Statistics View.
- 📊 The Load over Time Statistics Settings page is used to configure the statistics module, the chart type and the chart properties of the Load over Time Statistics View.
- 🌐 The Report Settings page is used to configure the schedule, target

directory, and format of network traffic reports.

 The Report Data page is used to configure the statistics module and the contained data of network traffic reports.

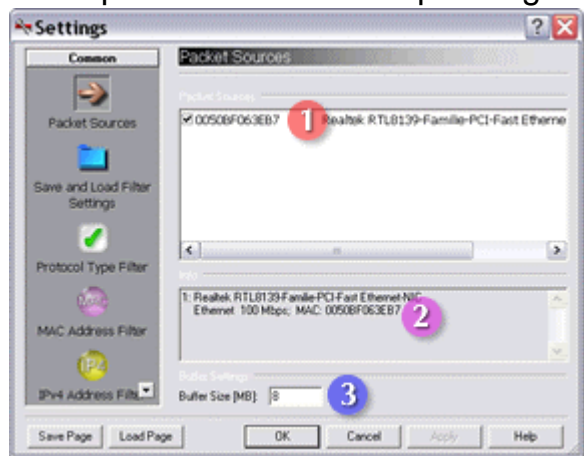
- 2 The title bar displays the name of the currently selected settings page.
- 3 This is the page area where the selected settings page is displayed.
- 4 The Save Page and Load Page buttons allow to save and load the settings of a single page to/from disk. If you want to save all your filter settings in a single file, use the Save and Load Filter Settings page of this dialog instead. The address filter pages will not save the address descriptions and colors in the file, as these are not part of the filter. If you want to save or load the address database, you will need to use the Export/Import Address DB commands in the File menu.
- 5 The OK button applies the settings and closes the dialog. The Apply button allows on some pages to apply your settings without closing the dialog. The Cancel button closes the dialog and dismisses all settings that were not applied yet. The Help button opens the context help for this dialog.

Note: Some settings are always applied immediately, thus you need not click Apply to do this, and the changes will not be dismissed if the Cancel button is clicked. These settings are address descriptions and colors, protocol colors, changes to the protocol groups tree, and changes to the Quick Load list of the Save and Load Filter Settings page.

5.2.1.1 Packet Sources



The Packet Sources page is part of the Settings dialog for capture filters. It is not present in the corresponding dialog for view filters.



- 1 The **Packet Sources** list contains all active network interface cards found on the system. The left column contains the MAC address of each card, the right column gives a short description. If more than one NIC is installed, you can choose from which cards to collect packets by checking or unchecking the entries. At least one entry must be checked. You can distinguish the packet sources of the collected packets in the Packet List View by means of the text color of the Time/Length information. The color can be changed in the Packet Source View.
- 2 The **Info** text box displays additional information for each network interface card in the list above.
- 3 The **Buffer Settings** edit box allows to change the buffer size of the packet store. If you open this page for an existing document, this box will be read only.

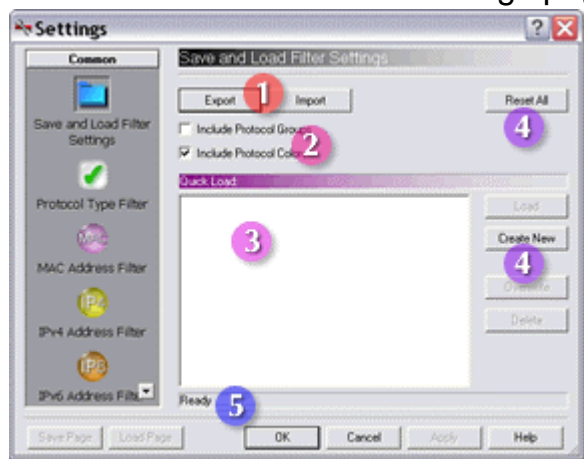
Please notice that you set the net size of the buffer. The actual demand of memory will be about 50% higher. This is due to internal memory management and address cache requirements.

Therefore the sum of the buffer sizes of all open documents should not exceed about one third to one half of your system's memory.



5.2.1.2 Save and Load Filter Settings

The Save and Load Filter Settings page inside the Settings dialog:



You can use this dialog to save and load filter settings either internally using the Quick Load list or externally to / from disk.

- 1 The **Export** and **Import** buttons allow to save and load your filter settings to / from disk. Usually it is more convenient to use the Quick Load list (see 3 and 4), but saving your settings to disk makes it possible to share settings between Network Analyzer instances on different computers.
- 2 These check boxes are used to include protocol groups and/or protocol colors (see Protocol Filter Settings) when you save or load filter settings.

They work for export and import as well as for quick load and save. This way you can assure that other users, who import your filter settings, will not destroy their own group and color settings. On the other hand you can create different protocol group settings and color schemes for different filtering applications. To create a file containing only the protocol group and color settings, check the Include boxes and click the Reset All button before saving the settings file.

Note: Address names and colors are not included in the filter settings files as these are not supposed to be part of the filter. The address database can be exported or imported with the corresponding File menu commands (see Exporting the address database).

- 3 The **Quick Load** list contains a number of filter settings that can quickly be loaded by double-clicking an entry or via the Load button on the right. You can edit the name of a selected entry by clicking it or by pressing F2 or Insert on the keyboard. Press Enter to finish editing or Esc to cancel.
- 4 The **Reset All** button resets all filter settings so that all packets will pass the filter.
The **Load** button loads the filter settings of the entry that is currently selected in the Quick Load list. The **Create New** button creates a new entry in the Quick Load list containing the current filter settings. The **Overwrite** button overwrites the selected Quick Load entry with the current filter settings. The **Delete** buttons deletes the currently selected entry in the Quick Load list.
- 5 The status bar displays information about the last accomplished action.

Note: You can save and load the settings of each individual page with the Save Page and Load Page buttons at the bottom of the Settings dialog.



5.2.1.3 Protocol Filter Settings

The Protocol Type Filter Settings page inside the Settings dialog:



- 1 The **Protocol Groups** tree contains a subset of protocol entries from the protocols list on the right. It is used to organize protocols in a hierarchical structure and allows to check or uncheck them in groups. To check or uncheck items click the icon on the left of an entry or select an item and press the spacebar on the keyboard. You can also use the context menu to check and uncheck groups. The context menu opens when you right-click an item. It offers also commands to create new groups and to delete protocol entries and groups.

If you right-click in an empty part of the tree view, the context menu will offer commands to create new top level groups and to check or uncheck all items of the tree view.

You can drag selected protocol entries from the protocols list into the tree view. If you drop them below the current tree, a new group containing the dropped protocols will be created. If you drop the entries into an existing group, they will be added to this group. Pressing the Ctrl button on the keyboard while dropping the entries will force the creation of a new subgroup containing the dropped protocol entries.

You can edit the name of a selected group by clicking it or by pressing F2 or Insert on the keyboard. To finish editing, click outside the edit box or press Enter on the keyboard. Press Esc on the keyboard to cancel editing. The group icon reflects the amount of selected items in the group and all of its subgroups by displaying a kind of pie-chart.

- 2 The **Protocols** list contains all protocols and packet types which can be used for filtering. The protocols are added to this list either internally, by decoder DLLs, or with configuration files for specific decoders. The list contains two additional columns that display an internal decoder

name or the name of a decoder DLL and the corresponding version date for some of the protocol entries. Protocol entries with an associated decoder will display more information in the Decode View.

You can sort the list in ascending or descending order by clicking once or twice into the list header.

To find a specific protocol entry, scroll the list or select any item and press the first letters of the searched protocol name on the keyboard. You can check or uncheck one or multiple selected entries to enable or disable these protocols in the protocol filter. If you want to check or uncheck some protocols frequently, it will be more convenient to add them to the group tree (see above).

- 3 The **Check all** and **Uncheck all** buttons are used to check or uncheck all protocol entries at once.

Note: If you uncheck all protocols, you need afterwards to enable the complete protocol stack used by the packets you want to pass through the filter (e.g. usually you won't see any packet as long as Ethernet is disabled). Notice that some protocols are further divided into sub-protocols which must all be enabled. Example: To see DNS packets, you need to check Ethernet, Ethernet II, IP, IPv4, UDP and DNS.

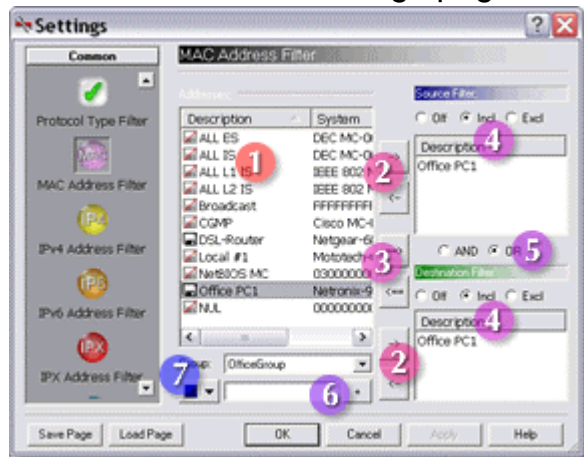
- 4 The foreground color button (**FG**) is used to change the text color of the protocol name in the Packet List View.
- 5 The background color button (**BG**) is used to change the background color of packet information text in the Packet List View. The background color is inherited by protocols that are contained or transported in a 'colored' protocol. If you assign a background color to the IP protocol, all packets using IP (including TCP, UDP, HTTP, etc.) will be displayed using this background color, as long as no other color is assigned to one of the upper protocols.

Note: This is used in the default configuration to highlight TCP connection management packets: TCP Synch (connect) packets have a green background, TCP Reset packets use yellow and TCP Final packets are displayed with a light red background. As these colors are inherited, this works for HTTP, POP3, and any other protocol using TCP.



5.2.1.4 Address Filter Settings

The Address Filter Settings page inside the Settings dialog:




This is the MAC Address Filter page, but the other address filter pages have the same layout.



- 1 The **Addresses** list contains three columns with different name formats for each address. The right column shows the raw name of the address, the middle column contains names with added system information, and the left column contains user editable descriptions. The name formats depend on the type of addresses handled by the actual filter dialog (see Address Name Formats for more information). To edit a description, select an address name in the first column, then click it a second time or press F2 or Insert on the keyboard. To accept the changes click outside the edit box or press Enter on the keyboard. To cancel editing press Esc on the keyboard. Addresses are added to the address database automatically while packets are collected or by using the edit box below the list (see 6).

You cannot delete addresses from this list while the application is running. But you can specify whether address information will be saved or not when the application is closed. The current state is revealed by the disk icons on the left of the address names. A strikethrough disk symbol refers to address entries that will be discarded, while address entries marked by a dark disk will be saved on disk. To toggle the persistence state, click the disk symbol or press the space bar on the keyboard while one or more entries are selected.

Note: Changes to the address descriptions, colors, and persistence states are applied immediately and won't be undone if you click the Cancel button. The Cancel button is only used to cancel address filter changes.

- 2 These buttons add or remove addresses to / from the Source or Destination filter. The right arrow button will add all selected entries from

the address list to the filter. The left arrow button  removes all entries selected in the respective filter list. If none is selected, it will remove all entries from the list. To remove a single address entry from one of the filter lists you can also double-click it.

- 3 These buttons add or remove addresses to / from the Source and Destination filter at the same time. The right arrow button  will add all selected address entries from the address list to both filter lists. To add a single address entry to both lists you can also double-click it. The left arrow button  is used to remove addresses from both filter lists.
 - If you selected entries in both lists, all selected entries are removed.
 - If you selected entries in only one list, these and the same entries in the other list are removed.
 - If no entry was selected, all entries from both lists are removed.
- 4 The **Source Filter** and **Destination Filter** lists with Include / Exclude selector buttons. If **Off** is selected, all packets will pass the filter ignoring the contents of the filter address list as if this filter does not exist at all. This means that the other filter (either destination or source) will get the full control if it is not switched off, too. If the filter address list is empty, the filter is implicitly switched off.

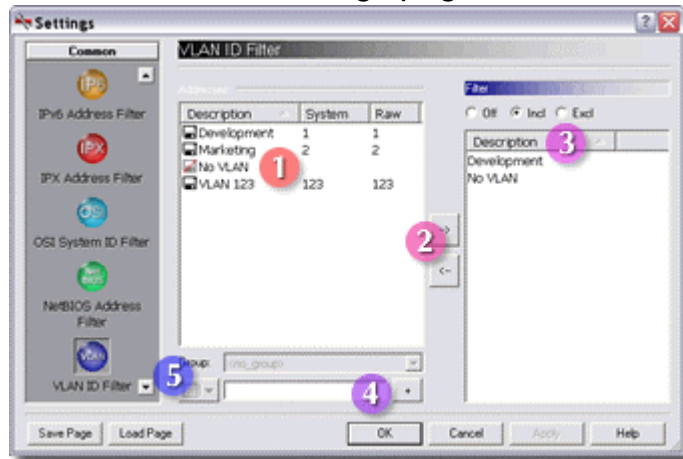
If **Incl** is selected, only packets containing an address from the list as source or destination address (depends on the corresponding filter list) will pass the filter. And if **Excl** is selected, only packets that do not contain an address from the list as source or destination will pass the filter. See also Address Filter Examples and Tips for more information.
- 5 The logical linkage between the source and destination filter. See Address Filter Examples and Tips.
- 6 This is an edit box to add new addresses to the address database. The address format to use here depends on the actual address filter page. See Address Name Formats. After entering the address, click the + button to add it to the list.
- 7 These are a color selector button and an address group combo box. Click the color selector button to open a color selection dialog to change the color of the address name in the Packet List View and Statistics View. You can choose Default in this dialog to remove the color information from the address entry. Use the address group combo box to assign the selected addresses to an address group. You can create new address groups on the Address Groups page of the Settings dialog.

Note: If you change any address information like description or color, the address entry will automatically become persistent; so your changes won't be lost on closing the application.



5.2.1.5 VLAN Filter Settings



The VLAN Filter Settings page inside the Settings dialog:





The VLAN ID Filter page has almost the same layout as the address filter pages, though it has only a single filter list as data packets always belong to one VLAN. As sender and receiver must be in the same VLAN, there is no need for a source and destination filter.

- 1 The VLAN ID list contains all known VLAN IDs. It has three columns as the address filter dialogs, though the Raw and System name for VLAN IDs are currently identical. To edit a description, select a VLAN ID name in the first column, then click it a second time or press F2 or Insert on the keyboard. To accept the changes click outside the edit box or press Enter on the keyboard. To cancel editing press Esc on the keyboard. VLAN IDs are added to the address database automatically while packets are collected or by using the edit box below the list (see 4).

The 'No VLAN' entry is a default name for packets that do not belong to a VLAN (normal LAN packets). You can use this value in the filter to include or exclude the normal network traffic without VLAN ID. If you like, you can change this name as any other VLAN ID name.

You cannot delete VLAN IDs from this list while the application is running. But you can specify whether VLAN ID information will be saved or not when the application is closed. The current state is revealed by the disk icons on the left of the VLAN ID names. A strikethrough disk symbol  refers to VLAN ID entries that will be discarded, while entries marked by a dark disk  will be saved on disk. To toggle the persistence state, click the disk symbol or press the space bar on the keyboard while one or more entries are selected.

Note: Changes to the VLAN ID descriptions, colors, and persistence states are applied immediately and won't be undone if you click the Cancel button.

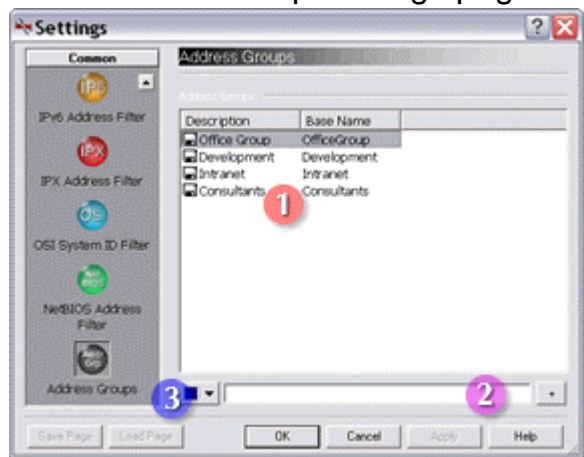
- 2 These buttons add or remove VLAN IDs to / from the filter list. The right arrow button  will add all selected entries from the address list to the filter. To add a single VLAN ID to the list, you can also double-click it. The left arrow button  removes all selected entries in the filter list. If none is selected, it will remove all entries from the list. To remove a single VLAN ID from the filter list you can also double-click it.
- 3 The **Filter** list with Include / Exclude selector buttons. If **Off** is selected, all packets will pass the filter ignoring the contents of the filter address list as if this filter does not exist at all. If the filter list is empty, the filter is implicitly switched off.
If **Incl** is selected, only packets that belong to a VLAN in the filter list will pass the filter. And if **Excl** is selected, only packets that do not contain a VLAN ID from the list will pass the filter. Use the 'No VLAN' entry to filter packets that do not belong to a VLAN at all (normal LAN traffic).
- 4 This is an edit box to add a new VLAN ID to the address database. Enter a number between 1 and 4095 and click the + button to add it to the list. See also Address Name Formats.
- 5 These are a color selector button and an address group combo box. Click the color selector button to open a color selection dialog to change the color of the VLAN ID in the Packet List View and Statistics View. You can choose Default in this dialog to remove the color information from the VLAN ID entry. Use the address group combo box to assign the selected VLAN IDs to an address group. You can create new address groups on the Address Groups page of the Settings dialog.

Note: If you change any VLAN ID information like description or color, the VLAN entry will automatically become persistent; so your changes won't be lost on closing the application.





5.2.1.6 Address Group Settings

The Address Group Settings page inside the Settings dialog:



The Address Group Settings page is used to create and manage address groups. You can assign addresses to these groups on the different Address Filter Settings pages inside the Settings dialog. Address groups can be displayed in the Packet List by adding the MAC Grp. or Layer 3 Grp. columns on the Packet List Columns Settings page. And you can use Address Group statistics modules for the Statistics View, the Load over Time Statistics View, and for Reports.

- 1 The **Address Groups** list contains two columns with different name formats for each group. The right column shows the raw name of the address group that was used when creating the group. This is also the name that is displayed in the Group combo box of the Address Filter Settings pages. The left column contains editable descriptions that can be used for more detailed information about an address group. You can display either format in the Packet List and the Statistics View. To edit a description, select an address group name in the first column, then click it a second time or press F2 or Insert on the keyboard. To accept the changes click outside the edit box or press Enter on the keyboard. To cancel editing press Esc on the keyboard. Addresses groups are added to the address database by using the edit box below the list (see 2). You cannot delete address groups from this list while the application is running. But you can specify whether address group information will be saved or not when the application is closed. The current state is revealed by the disk icons on the left of the address group names. A strikethrough disk symbol  refers to address group entries that will be discarded, while address group entries marked by a dark disk  will be saved on disk. To toggle the persistence state, click the disk symbol or press the space bar

on the keyboard while one or more entries are selected.

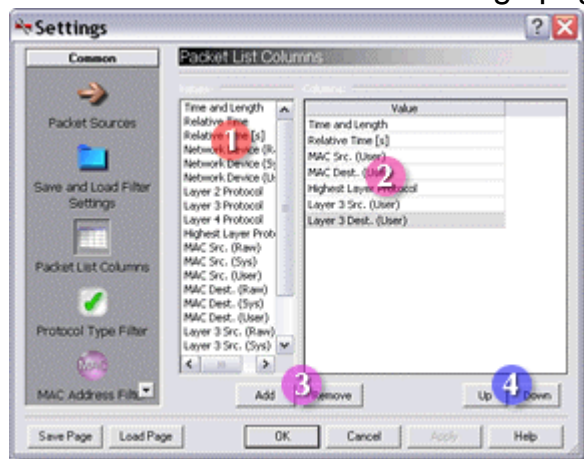
Note: Changes to the address group descriptions, colors, and persistence states are applied immediately and won't be undone if you click the Cancel button.

- 2 This is an edit box to add new address groups to the address database. After entering the address group name, click the + button or press the Enter key to add it to the list.
- 3 This is a color selector button. Click it to open a color selection dialog to change the color of the address group name in the different views and in reports. You can choose Default in this dialog to remove the color information from the address group entry.



5.2.1.7 Packet List Columns Settings

The Packet List Columns Settings page inside the Settings dialog:



Note: This page is available in both the capture settings dialog and the view filter dialog. If you modify your column settings in the view filter dialog, the changes will only be applied to the current view. If you opened additional views via the Windows menu, you can change the column settings of all views at once by using the capture settings dialog to modify the column settings.

- 1 The **Values** list contains all available values (columns) that can be displayed in the Packet List View. To add values to the column list, select one or more items and click the Add button. To add a single value, you can also double-click it. The new values will be added to the column list after the currently selected column. See also Packet List Columns for an overview of the available column types.
- 2 The **Columns** list contains the selected value columns that will be displayed in the Packet List View. To remove columns, select one or more

rows and click the Remove button. To change the sequence of value columns use the Up and Down buttons.

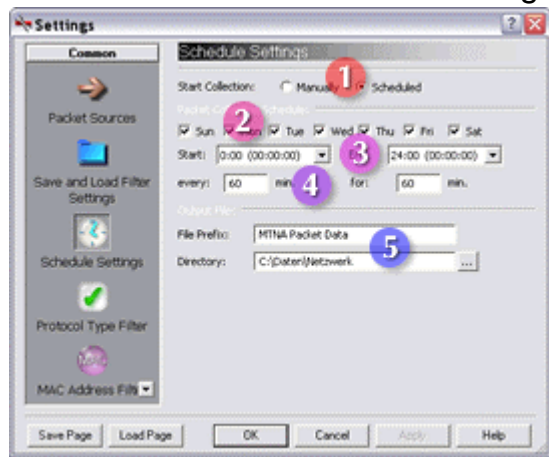
- 3 The **Add** button will add all selected display values in the value list to the column list on the right. The **Remove** button will remove all selected rows from the column list.
- 4 The **Up** button moves a selected row in the column list one position up. This means that the corresponding column in the Packet List View will be moved one position to the left. The **Down** button moves a selected row one position down.



5.2.1.8 Scheduled Packet Capture Settings

(PRO VERSION)

The Scheduled Packet List Settings page inside the Settings dialog:



Use this page to set the schedule and directory for capturing network data that you don't want to analyze immediately.

- 1 You can choose here to start and stop capturing data manually or via the integrated scheduler.
- 2 Use the day of week check boxes to enable or disable capturing of data on the corresponding days.
- 3 The **Start** time sets the time when the first data file will be created. The **End** time indicates the time on and after which no new packet data files will be captured on the same day. So if you set 10:00 as start time and 12:00 as end time for capturing data that is started every 60 min. for 60 min., you will get 2 data files every day. One running from 10:00 till 11:00 and one running from 11:00 till 12:00. If you use the same period for 45 min. captures that are started every 45 min., you will get 3 files (10:00-10:45, 10:45-11:30, 11:30-12:15).
- 4 Here you set the frequency for creating new data files (**every** ... minutes) and the duration of each capture (**for** ... minutes). The capturing schedules

may overlap (e.g. start a new file every 30 minutes for 60 minutes).

Note: If you start capturing via the command line together with the one-time (-o) option, all schedule settings except for the duration will be ignored (see Scheduled Packet Capturing).

- 5 The **File Prefix** will be used together with the start time and date when the data file is saved to disk. The format of the filename is: '[File Prefix] YYYY-MM-DD HHhMM.txt' (e.g.: 'Network Data 2007-02-01 10h00.txt' for a file that was started on February the 1st, 10:00). This format of date and time ensures a chronological order of the files in alphabetical sorted explorer windows or directory listings.

In the **Directory** edit box you can set the directory in which the reports will be stored. If the directory does not exist, it will be created when the first file is created. Click the button on the right to open a directory selection dialog.



5.2.1.9 Statistics Settings

The Statistics Settings page inside the Settings dialog:



- 1 The **Statistics Module** combo box contains all available statistics modules. You can use the **Module Filter** combo boxes to limit the number of statistics modules that are displayed in the Statistics Module drop list. If you change the statistics module, the value list on the left will be updated to contain all available display values (columns) for the new statistics module. If you select a statistics module of the same group, the list of columns (on the right) will not change, otherwise it will be filled with the values that were selected the last time this module was used.
- 2 The **Values** list contains all available values (columns) that can be displayed by the currently selected statistics module. To add values to the column list, select one or more items and click the Add button. To add a single value, you can also double-click it. The new values will be added to the column list after the currently selected column.

3 The **Columns** list contains the selected value columns that will be displayed in the Statistics View. To remove columns, select one or more rows and click the Remove button. To change the sequence of value columns use the Up and Down buttons.

You can also change the display format for the values here. Open a list of available formats with the little arrow buttons in the format column. You can choose between the following formats:

- Text: The values will be displayed in text format.
- Small Bar: Values will be displayed as narrow bar graph. The value is also displayed in text format in the center of the bar. Use this format together with a small font (about 7 point).
- Small Bar(%): Same as Small Bar, but the value is displayed as percentage of the Min Max difference. The Min and Max values can be changed in the corresponding columns to the right.
- Bar: Same as Small Bar but wider. Use this format together with larger fonts (about 10-12 point) or the system font.
- Bar(%): Same as Small Bar(%) but wider.

Note: Text-only values like addresses or protocol names will always be displayed as text. Also the color setting is not used for text display but only for bar graphs. Addresses will be displayed using the color that was selected via the Address Filter Settings page of the Settings dialog or the Edit Address Information Dialog. Protocol names will use the text color that was assigned on the Protocol Filter Settings page (foreground color only).

The following columns in the table are only relevant if you selected a graphic format for the value display. In this case you can edit the value's minimum and maximum. This will be used to calculate the filled area of the bar graphs and the percentage display. The minimum value will usually be zero. The maximum value depends on the unit of the chosen display value and your network speed. So if a value is displayed as MBit/s and your computer is attached to a 10 MBit LAN the maximum value will be 10. If you want to display the KByte/s rate of a 54 MBit WLAN the maximum value will be $54 / 8 * 1024 = 6912$ KByte/s. To edit these values select the corresponding table cell and press F2 or Insert on the keyboard, edit the value, and press Enter.

The last column allows to edit the color of the bar graph. Click the '...' button to open a color selector.

4 The **Add** button will add all selected display values in the value list to the column list on the right. The **Remove** button will remove all selected rows from the column list.

5 The **Up** button moves a selected row in the column list one position up. This means that the corresponding column in the Statistics View will be moved one position to the left. The **Down** button moves a selected row

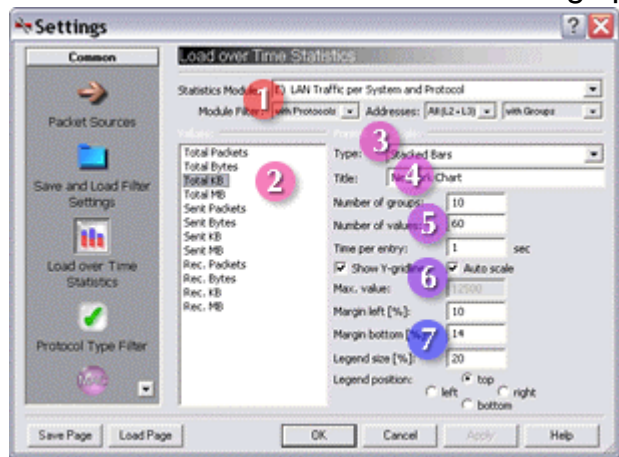
one position down.



5.2.1.10 Load over Time Statistics Settings

(PRO VERSION)

The Load over Time Statistics Settings page inside the Settings dialog:



- 1 The **Statistics Module** combo box contains all available statistics modules. You can use the **Module Filter** combo boxes to limit the number of statistics modules that are displayed in the Statistics Module drop list. If you change the statistics module, the value list on the left will be updated to display the types of values that can be used for the Load over Time Statistics.
- 2 The **Values** list contains all available types of values that can be displayed by the currently selected statistics module in the Load over Time Statistics. You need to select exactly one entry in this list.
- 3 The Chart **Type** combo box allows to select the chart type that shall be used to display the Load over Time Statistics. See Load over Time Charts for more information about the available chart types.
- 4 The Chart **Title** will be displayed together with the current time below the X-axis of the chart.
- 5 Here you can edit the **Number of groups** of values that shall be displayed in the chart (2-10). This is the number of lines in a line chart, the number of stacked sub-bars per bar in a stacked bar chart, or the number of bars per group in a group bar or deep bar chart. Please note that always one value group ('other') is used to display data traffic that could not be assigned to one of the visible groups (this includes possible rounding differences).

Note: The Network Analyzer will always show the data groups that caused the most traffic over the time that is displayed in the chart. Therefore all captured data for the displayed period is summed up and sorted every time

a new entry is added to the chart. So if you choose to display 6 groups in the chart, you will get the top 5 traffic causers and the 'other' group.

The **Number of values** is the number of points per line, of bars, or of groups of bars in a chart.

The **Time per entry** is the number of seconds that are used to capture data for each new entry in the chart. The chart will always display the cumulated data traffic that was measured during this period (e.g. Total kilobytes per 5 seconds), not a normalized value.

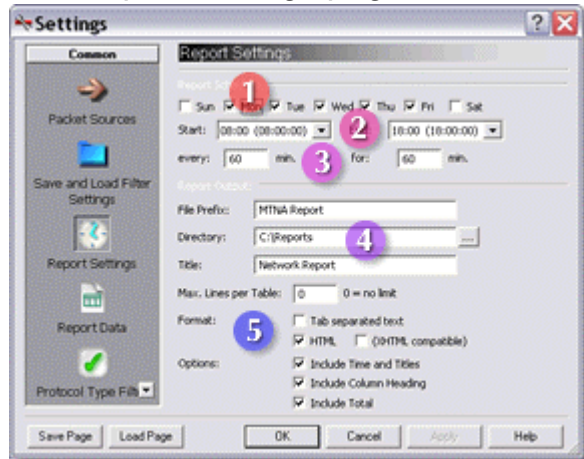
- 6 These controls allow to edit the properties of the Y-axis. Use **Show Y-gridlines** to display horizontal gridlines in the chart. If **Auto scale** is checked, the Y-axis will be automatically rescaled if a value is added to the chart that is greater than the current maximum. If Auto scale is not checked, you can enter the maximum value for the Y-axis in the **Max. value** edit box. The latter is useful if you know the maximum throughput of the monitored network and want to see the used and free bandwidth.
- 7 Here you can control the chart margins and legend position.
 - Use **Margin left** to edit the space between the Y-axis and the left window border in percent of the window width (1-45%). This space is used to display the axis labels and the Y-axis lettering.
 - Use **Margin bottom** to edit the space between the X-axis and the lower border of the window in percent of the window height (1-45%). This space is used to display the axis labels and the chart title. You may need to increase either margin values for small window sizes.
 - With **Legend size** you can change the space between the chart border and the window border on the side of the window where the legend is positioned. You can use values between 5% and 50% of the window size. If some of the legend labels are very long, you may also need to resize your window to avoid an overlapping of legend and chart.
 - The **Legend position** options control the position of the legend in the chart window: The **top** option places the legend above the chart, the **bottom** option places the legend below the chart. If possible, multiple labels will be displayed in a single line. If many long labels are displayed, the legend may overlap the chart or some labels may not fit into the window. Try to increase the window width in this case. The **right** and **left** options place the legend right or left of the chart. Very long labels may overlap the chart (left) or may be truncated (right). Use greater legend sizes in this case.



5.2.1.11 Report Settings

(PRO VERSION)

The Report Settings page inside the Settings dialog:



Use this page to set the schedule, directory, and format of a report.

Additionally go to the Report Data page to configure the contents of the report.

- 1 Use the day of week check boxes to enable or disable the generation of reports on the corresponding days.
- 2 The **Start** time sets the time when the first report will be started. The **End** time indicates the time on and after which no new report will be started on the same day. So if you set 10:00 as start time and 12:00 as end time for reports that are started every 60 min. for 60 min., you will get 2 reports every day. One running from 10:00 till 11:00 and one running from 11:00 till 12:00. If you use the same period for 45 min. reports that are started every 45 min., you will get 3 reports (10:00-10:45, 10:45-11:30, 11:30-12:15).
- 3 Here you set the frequency for starting reports (**every** ... minutes) and the duration of each report (**for** ... minutes). Report schedules may overlap (e.g. start a report every 30 minutes for 60 minutes).

Note: If you start a report via the command line together with the one-time (-o) option, all schedule settings except for the duration will be ignored (see Advanced Report Topics).

- 4 The **File Prefix** will be used together with the start time and date when the report is saved to disk. The format of the filename is: '[File Prefix] YYYY-MM-DD HHhMM.txt' (e.g.: 'MTNA Report 2003-11-01 10h00.txt' for a report that was started on November the 1st, 10:00). This format of date and time ensures a chronological order of the files in alphabetical sorted explorer windows or directory listings.

In the **Directory** edit box you can set the directory in which the reports will

be stored. If the directory does not exist, it will be created when the first report is started. Click the button on the right to open a directory selection dialog.

The **Title** will be used as title for the generated reports. If you do not want to have a title, leave the edit box empty.

- 5** The **Max. Lines per Table** edit box allows to limit the lines of data that will be contained in the report tables. Set this value to zero to disable the line limit and to include all data in the report.

Use the **Format** options to set the report format. Choose **Tab separated text** for plain text reports that can be easily imported into other applications. Choose **HTML** to generate an appealingly formatted report that also may contain charts (see Report Data). The style of HTML reports can be modified (see Advanced Report Topics). You can choose to generate XHTML compatible reports by checking the **XHTML compatible** option.

The **Options** section allows to switch report details on and off. **Include Time and Titles** will add the report running time and the used statistics modules to the report. **Include Column Heading** adds a heading row to the data tables. And **Include Total** will add a row with the sum of all collected data to the tables.

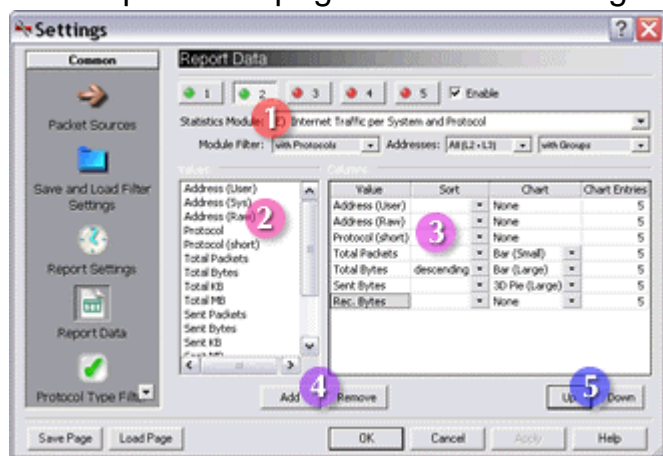
Note: The 'Total' row will actually display the total of the collected data and not the column sum! Due to table line limitation (see above) and rounding errors these values may be different.



5.2.1.12 Report Data

(PRO VERSION)

The Report Data page inside the Settings dialog:



You set the contents of a report on this page. Use the Report Settings page to configure the schedule and directory of the report.

- 1 You can create reports with multiple tables and charts. The buttons at the top of the dialog page are used to select the table that you want to configure. To include a table in the report, you need to check the **Enable** box on the right. Currently enabled tables are marked with a green LED on their button. Tables that are marked with a red LED will not be included in the report.

The **Statistics Module** combo box contains all available statistics modules that can be used for reports. You can use the **Module Filter** combo boxes to limit the number of statistics modules that are displayed in the Statistics Module drop list. If you change the statistics module, the value list on the left will be updated to contain all available display values supported by the new statistics module. If you selected a statistics module of the same group, the list of columns (on the right) will not change, otherwise it will be filled with the values that were selected the last time this module was used.

- 2 The **Values** list contains all available values (columns) that can be contained in a report table with the currently selected statistics module. To add values to the column list, select one or more items and click the Add button. To add a single value, you can double-click it as well. The new values will be added to the column list after the currently selected column.
- 3 The **Columns** list contains the selected value columns that will be contained in the generated report table (see also Generating Reports). To remove columns, select one or more rows and click the Remove button. To change the sequence of value columns use the Up and Down buttons. In the sort column of the table you can select by which column the reported data will be sorted and whether to use ascending or descending order. This setting is particularly important if you limited the number of lines per table for the report on the Report Settings page. If no column is selected for sorting the report will contain the data in the order it was received from the network. If you include the column headings in the report, the name of the column that was used for sorting will be marked with a little arrow: (^) for ascending order or (v) for descending order.

Optionally you can add a chart for every column that contains numerical data (charts will not be generated for text-only reports - see Report Settings). The chart type and size are selected in the Chart column (see Report Charts for more details). In the Chart Entries column you can select the maximum number of bars or pie slices that the chart will display. The values in the chart will always be sorted in descending order.

Note: The maximum number of bars or pie slices per chart is fifteen. If more data was collected the chart will contain an additional bar or slice labeled 'Other' that shows the sum of all other data values that are not displayed. Also pie charts will only display values that exceed 3% (large pie chart) or 5% (small pie chart) of the total values, as otherwise the

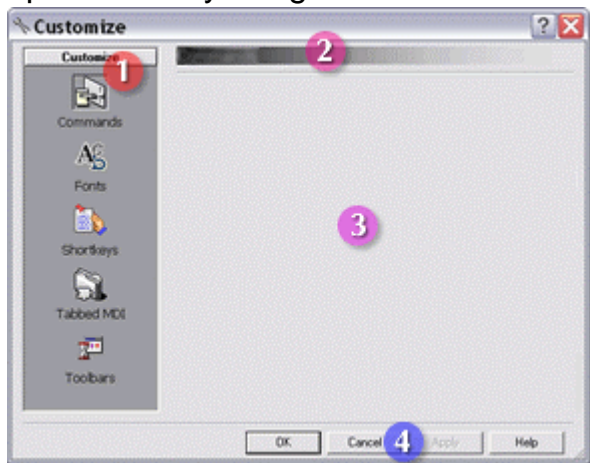
labels would overlap.

- 4 The **Add** button will add all selected display values in the value list to the column list on the right. The **Remove** button will remove all selected rows from the column list.
- 5 The **Up** button moves a selected row in the column list one position up. This means that the corresponding column in the report will be moved one position to the left. The **Down** button moves a selected row one position down.



5.2.2 Customize Dialog



You can use the Customize dialog to customize the user interface of the Network Analyzer application to fit your needs. It is opened with the Customize command in the Tools menu or with the context menu that opens when you right-click the toolbar or menu area.






Please note that new versions of the Network Analyzer will not always be able to preserve your customizations.

- 1 The page list contains entries for all available customization pages. If not all items are visible in the list, you can either resize the dialog, scroll the list up or down with the small arrow buttons at the top and bottom, or you right-click the list to get a context menu that offers commands to change the size of the icons.

Following pages are available:

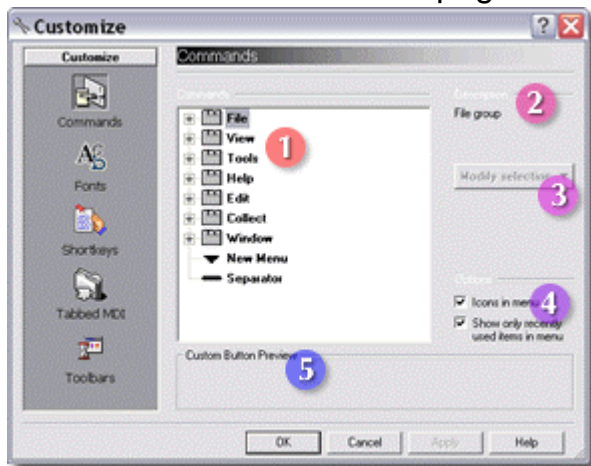
-  The Commands page is used to customize menus and toolbars and to create additional menus.
-  The Fonts page is used to change the fonts of the Packet List View, the Decode View, and the Hex View.

-  The Shortkeys page is used to add and change keyboard shortcuts to the Network Analyzer menu commands.
 -  The Tabbed MDI page is used to customize the look and behavior of the view window tabs in the main window.
 -  The Toolbars page is used to change the look of the toolbars and to create and manage new ones.
- 2** The title bar displays the name of the currently selected customization page.
 - 3** This is the page area where the selected customization page is displayed.
 - 4** The OK button applies the settings and closes the dialog.
The Apply button allows on some pages to apply your settings without closing the dialog.
The Cancel button closes the dialog and dismisses all settings that were not applied yet.
The Help button opens the context help for this dialog.



5.2.2.1 Customize Commands

The Customize Commands page inside the Customize Dialog:



While this dialog is open, you can drag commands from its commands tree directly into toolbars and menus of the application. You can also move command entries and buttons in toolbars and menus to other locations. If you press the Ctrl key while dragging an item, it will be copied. If you move an item outside of a toolbar or menu, it will be deleted.

- 1** Drag items from the commands tree into menus or toolbars of the application.
Drag the New Menu item into a menu bar to create a new menu there.
Click the Modify selection button afterwards to change the name of the new menu.

Drag the Separator item into menus or toolbars to create separators there. You can also create separators in toolbars by dragging a button slightly to the left or right. To remove a separator in a menu, select it and drag it out of the menu or use the Delete command of the Modify selection button. To remove a toolbar separator, drag the button beside the separator next to the button on the other side of the separator.

- 2 This is the description of the selected item in the commands tree. It is the same text as is displayed in the status bar while the mouse pointer hovers over a toolbar button or menu entry.
- 3 The Modify selection button allows to modify menu entries or toolbar buttons of the application. It does not modify items selected in the commands tree!

If a menu entry was selected, you can delete it or open a dialog via the Button Appearance command. In the dialog you can change the menu text. You can prefix one letter of the command text with a '&'. This will become the keyboard key that in combination with the Alt key allows to open the menu or execute the menu command. (Additionally you can create and modify keyboard shortcuts to your menu commands on the Shortkeys page.)

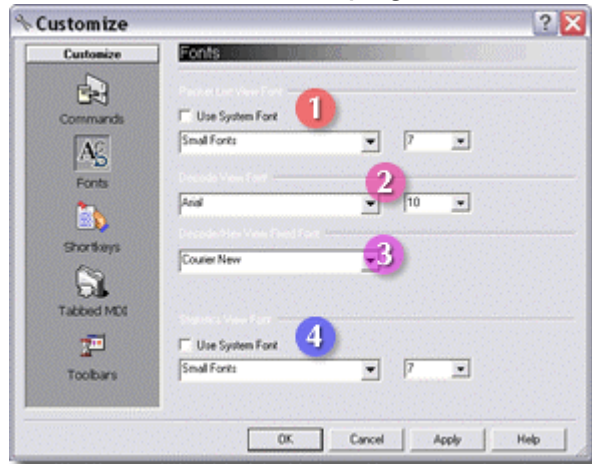
If a toolbar button was selected, the button displays some more commands in its menu. You can delete the button or open the button appearance dialog. You can select whether to display the button image with or without text, and you can add a separator before or after the button. In the appearance dialog you can change the button image and text.

- 4 Uncheck the 'Icons in menu' option to display text-only menus. If you check the option 'Show only recently used items in menu', some infrequently used menu entries will be hidden. To make hidden menu items visible, click the small arrow at the bottom of the menu.
- 5 The Custom Button Preview is not used as currently no custom buttons are present in the application.



5.2.2.2 Customize Fonts

The Customize Fonts page inside the Customize Dialog:



You can modify the fonts used by the Packet List View, the Decode View, the Hex View, and the Statistics View in this dialog.

- 1 The Packet List View will use the system font to display packet information if the **Use System Font** checkbox is checked. If you want to use other fonts, uncheck the **Use System Font** checkbox. Now you can choose a font with the font combo box and change its size with the size combo box on the right. After applying these changes, all Packet List Views will be updated immediately.

Note: If you want or need to use rather small fonts, you should select pixel fonts (e.g. the 'Small Fonts' font with a size of 6 or 7).

- 2 Change the standard font of the Decode View with the font combo box here. The size combo box on the right allows to change the font size of both the Decode View and the Hex View.

Note: If you apply changes to the Decode/Hex View fonts, the new fonts will be used the next time a packet is decoded.

- 3 This combo box is used to change the fixed-pitch font that is used in the Hex View and for some values in the Decode View.
- 4 The Statistics View Font can be changed here. As for the Packet List, you can choose to use the system default font by checking the **Use System Font** checkbox.



5.2.2.3 Customize Shortkeys

The Customize Shortkeys page inside the Customize Dialog:



You can assign new or remove present keyboard shortcuts to menu commands in this dialog. To assign a new shortcut, select a menu command in the Commands list, click inside the 'Press new shortcut key' edit box, press the key you want to assign on the keyboard, and assign it with the Assign button.

Note: The Network Analyzer documentation references some default shortcuts. So if you remove existing keyboard shortcuts, the application may not work anymore as described in the help file and manual.

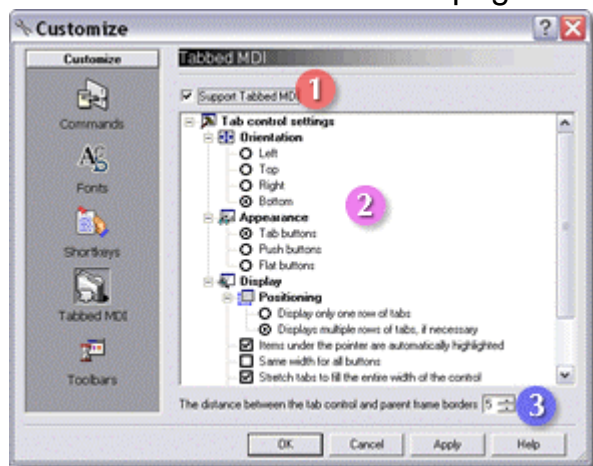
- 1 This tree view contains all menu commands of the application. Select a command entry here to modify its keyboard shortcuts.
- 2 The description of the currently selected item in the commands tree.
- 3 You can use this combo box to select whether a keyboard shortcut shall work everywhere in the application or only when specific views are active. Usually you needn't change anything here.
- 4 The Current keys list displays the keyboard shortcuts that are currently assigned to the selected menu command.
- 5 These buttons allow to assign a new shortcut (see 6) to the selected menu command or to remove the selected or all shortcuts from the Current keys list.
The Reset All button will reset all keyboard shortcuts to the values they had when the dialog was opened. In contrast to the Cancel button, this will reset also changes that were already applied with the Apply button.
- 6 This edit box is used to enter new keyboard shortcuts. Activate it and press any key on the keyboard (e.g. Ctrl+X). If the shortcut is already assigned to another menu command, you will get a warning in the Conflict text box (7).

- 7 This text box will display a warning if you try to assign a keyboard shortcut that is already in use.



5.2.2.4 Customize Tabbed MDI

The Customize Tabbed MDI page inside the Customize Dialog:



With this dialog you can control the appearance of the main window's view tabs. By default you will see a row of tabs near the bottom of the main window that can be used to quickly switch between different windows inside the mainframe of the application window.

- 1 The '**Support Tabbed MDI**' checkbox allows to deactivate and hide the tabs altogether.
- 2 The **Tab Control Settings** change the appearance of the tabs in the main window:
 - ✚ The **Orientation** options control the side of the window to which the tabs are attached.
 - 🖼 The **Appearance** options are used to change the look of the tabs. You need to uncheck the 'Unused tabs move to the opposite side' option to use push buttons or flat buttons.
 - 🖼 The **Display** option controls the positioning of the tabs and their label text.

Following options take only effect if there is not enough space to position all tabs in one row:

- **Display only one row:** Arrow buttons are displayed to scroll the view to tabs, which are currently not visible.
- **Display multiple rows:** The tabs are placed in multiple rows one upon the other.
- **Unused tabs move to the opposite side:** Tabs, that do not fit into the current row are moved to the opposite side of the window and placed in multiple rows there, if needed. Only the

tab of the current active view is guaranteed to stay on the side of the window, which was set in the orientation options.

To highlight the label text, when the mouse hovers over the button, check the corresponding option ('**Items under the pointer...**').

You can force a fixed width for all tab buttons by checking the '**Same width for all buttons**' option. If the label text is too long, it will be truncated.

The '**Stretch tabs to fill the entire width**' option allows to stretch the tab buttons to fill the whole window width. This will only work, if more than one row of tabs is currently displayed and if the 'Same width...' option is unchecked.

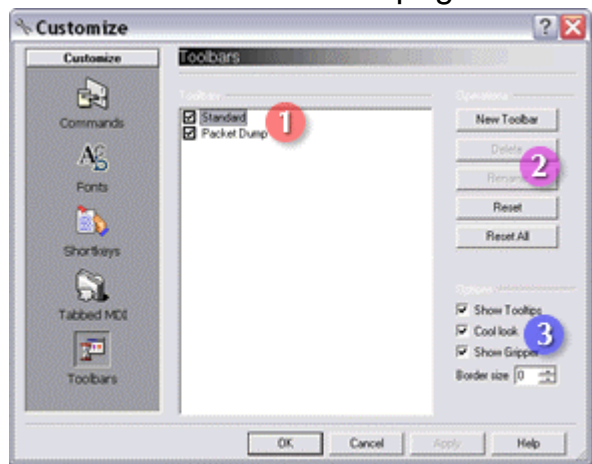
The last two '**Aligns...**' options will modify the positioning of label text and icon in the tab button, if the 'Same width...' option is checked.

- 3 This control allows to change the distance between the tabs and border of the parent frame.



5.2.2.5 Customize Toolbars

The Customize Toolbars page inside the Customize Dialog:



You can toggle the visibility and modify the look of existing toolbars in this dialog, and you can create and delete new toolbars here.

- 1 The Toolbars list contains all toolbars of the Network Analyzer application. Click the checkbox to toggle the visibility of the toolbars.
 - 2 You can add new toolbars here by clicking the New Toolbar button. This will add a new entry to the Toolbars list where you can then edit the name of the new toolbar. Click outside the edit box to finish editing. Afterwards you can use the Customize Commands page to add command buttons to the toolbar.
- If you select a toolbar that was created this way, you can rename and

delete it with the corresponding buttons. You cannot rename or delete the application's own toolbars.

If you added commands to the application's toolbars you can reset them to their initial state with the Reset or Reset All buttons. These buttons have no effect on user created toolbars.

3 These options change the look and behavior of the toolbars:

If you uncheck 'Show Tooltips', you won't get tooltips anymore, when the mouse hovers over a tool button.

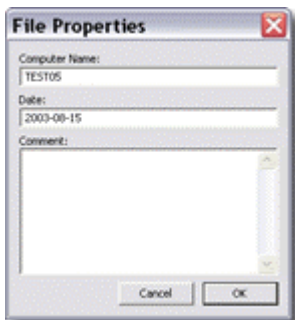
The 'Cool look' option toggles between flat and elevated look of the tool buttons.

The 'Show Gripper' option toggles the visibility of the gripper on the left of flat toolbars.

The 'Border size' control allows to increase the size of the tool buttons.



5.2.3 File Properties Dialog

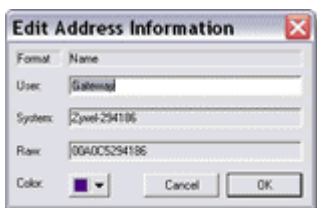


To open the File Properties dialog for the currently active document, use the Properties command in the File menu. The values for Computer Name and Date are assigned when the document is created, but you can change these values if you want.

You can also add a comment here. All values are saved in the document.



5.2.4 Edit Address Information Dialog



To open the Edit Address Information dialog, right-click an address in the Packet List View or Statistics View to display a context menu and then use its Properties command.

You can change the address description in the edit box and the address text color with the color selector button. Click the OK button to apply your changes or click Cancel to close the dialog and dismiss your changes.

Note: If you change something here and click the OK button, the corresponding entry in the address database will automatically become persistent. Thus your changes will be saved when the application is closed. Use the Address Filter Settings page to change the persistence state of your address database entries.

5.2.5 Color Selector



The Color Selector Popup window offers a palette of colors to choose from. It is used to change the colors of address and protocol information displayed in the Packet List View. Click any of the color boxes to select a color, or click default to use the default color (black for text or white for the background). You can also click the Custom button to open the standard color dialog of Windows and select a color not present in the palette.

You can change address text colors on the Address Filter Settings page of the Settings Dialog or in the Edit Address Information Dialog.

To change the protocol type text color or the background color, use the Protocol Filter Settings page.

The color of the Time/Length text can be changed in the Packet Source View for each network interface card. You may need to scroll the view content to see the Text Color buttons.

5.2.6 Register MTNA Dialog



Use the Help > Register Network Analyzer menu command to open the Register MTNA dialog. See Registration on how to register your copy of the MaaTec Network Analyzer.

MaaTec Network Analyzer

If you received a valid license key, enter your registration name in the upper edit box and the license key in the edit box below, then click OK.



5.2.7 About Box

? Click the About button ? or use the Help > About Network Analyzer menu command to open the About Box. The About Box displays version and license information and contains a link to the MaaTec Network Analyzer web site. You can see here the expiry date of demo versions. If your version has expired, you can use the Help > Register Network Analyzer menu command to open the Register MTNA Dialog and register your copy of the application.

If you are running the application with a trial license, you will see the demo-mode About Box:



You can switch between the Pro and the Std demo mode here. Therefore click the **Switch to Std-Demo** or **Switch to Pro-Demo** button. Please note that the application will continue to run in the current demo mode until you restart it. If you are running the standard demo and you switch to the Pro-Demo, the Network Analyzer needs to reset the menus and toolbars. This means that any GUI customizations will be reset as well.

If you have entered a valid license key, you will see an About Box without demo switching options:



5.3 Menus








5.3.1 File Menu




The File menu contains commands for file handling, address database export and import, and printing. You can close the application by using the Exit command, and you can open documents that were recently used. The names of these documents are listed in the recent file list inside the File menu. The **Properties** command opens the File Properties dialog.

5.3.1.1 File Handling



-  **New:** Use this command to create a new default document to collect network packets. This will open a ring buffer document with a packet list view. You can open additional views for this document by using the Window > New Window menu command.
Keyboard shortcut: Ctrl+N.
 -  **New Scheduled Collector:** Create a new Scheduled Capture View with this command. See Scheduled Packet Capturing for more information.
Keyboard shortcut: Ctrl+D.
 -  **New Statistics:** This command will open a new Statistics View, that will display information about the current network traffic. See 'Network Statistics' for an introduction.
Keyboard shortcut: Ctrl+T.
 -  **New Load over Time Statistics:** Open a new Load over Time Statistics View, that will display statistical information about the network traffic over a configurable period of time.
Keyboard shortcut: Ctrl+H.
 -  **New Report:** Create a new report generator with this command. See also: 'Generating Reports'.
Keyboard shortcut: Ctrl+R.
 -  **Open:** This command allows to load previously saved files from disk. You can choose the file in a standard file open dialog.
Keyboard shortcut: Ctrl+O.
- Close:** You can close a document with all its views with this command. If you want to close only a single view, use the close button  in the upper right corner of the view window.
Keyboard shortcut: Ctrl+F4.

 **Save:** Use this command to save a previously saved document in the same file again. If the document wasn't saved yet, a standard Save As dialog will be shown (see Save As).


Keyboard shortcut: Ctrl+S.

Save As: This command opens a Save As dialog. You can select a directory and a file name in this dialog, and you can set some additional options:

- **Save All:** All packets in the document will be saved in the file.
- **Save Filtered:** This option is only available if you applied a view filter to the current view. It will save all packets that are visible in the list view.
- **Save Selected:** This will save only the currently selected packets.
- **Compress:** The file will be compressed when saved, thus it will use less space on the disk.

5.3.1.2 Exporting the address database




You can export your address database into a file. Use therefore the File > **Export Address DB** command. This will export all address entries that are marked as persistent () including their color setting. The persistence state is set on the address filter pages of the Settings dialog.

To import an address database from disk, use the File > **Import Address DB** command. This will display a File Open dialog with additional options. You can select at the bottom of the dialog whether you want to retain or overwrite your current address settings if corresponding entries are found in the imported file. And you can decide to import the addresses temporary or persistent.

Depending on this setting, the persistence flag of imported address entries will be set.

5.3.1.3 Printing



 **Print:** This command is available if the cursor was placed inside the decode view or hex view. It will print the contents of the respective view.

Keyboard shortcut: Ctrl+P.

Print Preview: You can open a print preview window with this command.



As the Print command, the Print Preview command is only available if the cursor is currently placed inside the decode or hex view. The buttons on top of the window allow to print the content of the preview window, to select other pages, and to zoom in or out of the page display. Click the Close button to return to the normal view.

Print Setup: This command opens the configuration dialog for the default printer. You can select another printer here, and you can modify the settings of the selected printer.


5.3.2 Edit Menu



The Edit menu contains commands to copy text, to find text strings, and to set bookmarks in the packet list view.

5.3.2.1 Copying Text



 **Copy:** After you selected some text in the decode view or hex view, you can use this command to copy the selected text to the clipboard. This text can now be pasted into other applications (e.g. Word, notepad, etc.). You can also copy the contents of the packet list view as tab-separated list to the clipboard.

Keyboard shortcuts: Ctrl+C or Ctrl+Ins.

Select All: Place the cursor inside the decode or hex view and then use this command to select all text of the respective view. Afterwards you can copy the text to the Windows clipboard.

Keyboard shortcut: Ctrl+A.

5.3.2.2 Finding Text



Find: If the cursor is placed in the decode view or hex view, you can search for a text string in that view. The Find command will open a Search dialog that allows to enter the searched text string and some search options.

Keyboard shortcut: Ctrl+F.


Find Next: This command will search for the next occurrence of the text that was entered in the Search dialog (see Find command).

Keyboard shortcut: F3.

5.3.2.3 Bookmarks



You can set bookmarks in the packet list view via the Edit menu. That way you can quickly jump between packets that are most interesting to you.

 **Toggle Bookmark:** This command sets a bookmark for the first selected item in the packet list view. If this item already has a bookmark, the bookmark will be removed. Bookmarks are saved together with the packet data.

Keyboard shortcut: Ctrl+F2.

Next Bookmark: Use this command to jump to the next item in the list that has a bookmark.

Keyboard shortcut: F2.


Previous Bookmark: Jump to the previous item in the list that has a bookmark.


Keyboard shortcut: Shift+F2.

Remove all Bookmarks: Remove all bookmarks from the packet list.

5.3.3 Collect Menu




 **Capture Settings:** This command opens the Settings dialog for filters and for statistics and report settings. You can modify the capture filter and other settings for the active document there.

 **Start:** Use this command to start collecting packets into the active document.

Keyboard shortcut: F8.


 **Stop:** This command stops collecting packets into the active document.

Keyboard shortcut: Ctrl+F8.


 **Empty Buffer:** This command deletes all packets that are stored in this document.

5.3.4 View Menu




 **View Filter:** This command opens the Settings dialog for the view filter of the active view. You can use this dialog to create a new or modify an existing view filter.

Keyboard shortcut: F10.


 **Remove View Filter:** Use this command to remove a view filter from the active view.


Keyboard shortcut: Ctrl+F10.


 **Auto Scrolling:** Enable or disable the automatic scrolling of the packet list view with this command.

Set Relative Time Origin: This command will set the relative time of the first selected packet in the packet list to zero. All time values in relative time columns will be displayed relative to this packet's time. The packet list needs to have a relative time column, otherwise you won't see an effect (see Packet List Columns Settings).


Keyboard shortcut: Ctrl+0.

 **All Details:** Display all details of a decoded packet in the decode view.

 **Common Details:** Display only common details in the decode view.

 **Minimum Details:** Display only the most important details of a decoded packet in the decode view.

 **B/W output:** Toggle between color and black and white output in the decode view and hex view.

 **Visibility options** for toolbars, status bar, and the Packet Sources window: Use these commands to hide and show the toolbars, the status bar, and the packet sources window.

5.3.5 Tools Menu




Always on top: This command toggles the window positioning behavior. If 'Always on top' is enabled, the application window will stay in front of all other desktop windows even when it loses the window focus (when you activate another window).

Hide when minimized: If this option is enabled and you minimize the application windows, the application's taskbar button will be removed and an icon will be added to the system tray. Double-click the icon to restore the Network Analyzer window.

Easy Statistics Mode: This command toggles between an easy statistics mode and an advanced statistics mode. By default the easy statistics mode is enabled. It reduces the number of available statistics modules for the real-time statistics and the network load over time statistics and displays more comprehensible names for the modules. The advanced user can switch off this mode. This way it is possible to use many more statistics modules for more advanced uses (e.g. analyzing lower layer protocol distribution). But to use this mode, you should be familiar with usual network terms like layers and the different types of addresses that are used in a network.

Auto-Update Address DB: Usually the network analyzer will use the information from ethernet headers and DNS, NetBIOS-NS, and DHCP packets to add new addresses and address names to the address database. While this is very convenient for most analyzing tasks, it may increase the amount of required memory. If this is not desired (e.g. for long-term reports), this behavior can be switched off here. While the auto-update of the address database is switched off, any address that is not found in the database will be displayed with a default name (e.g. 'Internet (v4)' or 'LAN'). This will also reduce the size of reports and statistics lists.

Auto-Start Collection: If Auto-Start is enabled, the network analyzer will start collecting packets as soon as a new packet list or statistics window is opened. If this option is disabled, you need to use the Collect > Start command or click the Start collect button  in the toolbar to start collecting data.

Customize: This command opens the Customize dialog. You can use this dialog to modify multiple aspects of the Network Analyzer's GUI including menus, toolbars, and keyboard shortcuts.

5.3.6 Window Menu



New Window: Create an additional view for the active document. You can apply a different view filter to each view of a document.

Cascade: Cascades all view windows. The windows overlap each other.

Tile: Tiles all view windows. The windows are displayed one above the other.

Arrange Icons: Arranges all minimized view window icons at the bottom of the main window.

Window list: This a list of open view windows. Select one to activate it. You can also use the main window's view tabs or the keyboard shortcuts Ctrl+Tab or Shift+Ctrl+Tab to activate different windows.

5.3.7 Help Menu



Help Topics: Displays the Network Analyzer help file.

Quickstart: Jump to the Quickstart guide in the help file.

Show Tip of the Day: Toggle the display of tips at application startup on and off.

Register Network Analyzer: Opens the Register MTNA dialog. You can register your copy of the Network Analyzer there.

 **About Network Analyzer:** Displays the MTNA About Box.



5.4 Toolbars

The Network Analyzer has initially two toolbars:

















- The Standard toolbar offers command buttons for file handling, packet collection, printing, and copying.
- The Packet List toolbar offers commands for view filter assignment and decode output settings.

You can modify the existing toolbars on the Commands page of the Customize dialog, and you can create your own toolbars on the Toolbars page of that dialog.










5.4.1 Standard Toolbar



-  **New Packet List:** Create a new Packet List document and view.
-  **New Scheduled Collector:** Create a new Scheduled Packet Capture document and view.
-  **New Statistics:** Create a new Statistics document and view.
-  **New Load over Time Statistics:** Create a new Load over Time Statistics document and view.
-  **New Report:** Create a new Report Generator. See also: 'Generating Reports'.
-  **Open:** Open a Packet List document file on the disk.
-  **Save:** Save document data in a file on the disk.
-  **Capture Settings:** Show the Capture Settings dialog.
-  **Packet Sources:** Toggle the visibility of the Packet Sources window.
-  **Start Collect:** Start collecting packets from the network into the active document.
-  **Stop Collect:** Stop collecting packets from the network.
-  **Empty Buffer:** Delete all packets stored in the active document.
-  **Copy:** Copy selected text from the decode view or hex view.
-  **Print:** Print the contents of the decode view or hex view.
-  **About:** Show the About Box.
-  **Help:** Get help for main window elements (see More Help).

5.4.2 Packet List Toolbar



-  **Auto Scrolling:** Enable or disable the automatic scrolling of the packet list when packets are received from the network.
-  **View Filter:** Apply a view filter to the active view.
-  **Remove View Filter:** Remove the view filter from the active view.
-  **All Details:** Display all details in the decode view when decoding a packet.
-  **Common Details:** Display common details in the decode view.
-  **Minimum Details:** Display only the most important details in the decode view.
-  **Toggle B/W output:** Switch between color and black and white output in the decode view and hex view.

5.5 Documents and Views



Like most Windows applications, the MaaTec Network Analyzer uses a data managing concept known as document view model. A document is a data store, while views display the document's data to the user.

The Network Analyzer applications uses two types of documents:

- File-based documents contain packet data that was loaded from disk. You cannot start collecting data into a document that was loaded from disk. See [Saving and Loading Data](#) for more information.
- Ring buffer documents are created by the user. You can start collecting packets from the network into these documents. See [Collecting Packets](#) for more information.

Currently both document types support one view type: The Packet List View displays the packets stored in a document as a list. You can use the Window > New Window menu command to open additional views for a document. This is especially useful if you assign different view filters to each view.

5.6 Packet List Columns



You can customize the columns that are displayed in the Packet List (see [Packet List Columns Settings](#) for further details). In the following table you will find the different types of data columns that can be used in the Packet List.

Time and Length	This is the standard time column. It displays the receive time of a packet as local system time, its length in bytes, and if packets were lost, it displays the number of packets that were lost before this packet.
Relative Time	This column displays the relative time of a packet. The relative time is set to zero, when you start data collection of a Packet List view for the first time. You can change the relative time origin via the View > Set Relative Time Origin menu command or by pressing Ctrl+0 on the keyboard. This will set the relative time of the first selected packet in the packet list to zero. Packets that were received before this packet will be displayed with a negative relative time. You can choose between two different formats: 'Relative Time' displays the time as hours, minutes, seconds, and microseconds; 'Relative Time [s]' displays the time as seconds and microseconds.
Network Device	This column will display the MAC address of the local network card that received a packet. See Address Name Formats for the different format options for the Network Device column. Note: This column is most useful if you collect packets from multiple network cards and want to use the keyboard navigation feature of the Packet List view (see Analyzing Data). You can also distinguish packets that were received by different network cards based on the color of the time column text (see Packet Source View).
Layer 2 Protocol	This column displays the layer 2 (data-link layer) protocol that was used to encode the packet (e.g. Ethernet II or LLC).
Layer 3 Protocol	This column displays the layer 3 (network layer) protocol that was used to encode the packet (e.g. IPv4 or NetBIOS).
Layer 4 Protocol	This column displays the layer 4 (transport layer) protocol that was used to encode the packet (e.g. UDP, TCP - Data, NetBIOS - Datagram).
Highest Layer Protocol	This column displays the protocol on the highest identified layer that was used to encode the packet. This may be one of the lower layer protocols that is also displayed in the layer 3 or layer 4 columns or an

	upper layer protocol (e.g. POP3, SMB).
MAC Src.	This column will display the layer 2 MAC address of the system in your LAN that sent a packet. This may be the original sender of the packet or a gateway to another LAN or the internet. See Address Name Formats for the different format options for the source and destination address columns.
MAC Dest.	This column will display the layer 2 MAC address of the system in your LAN that shall receive a packet. This may be the final destination of the packet or a gateway to another LAN or the internet.
MAC Grp. Src./Dest.	These columns will display the address group to which a MAC address belongs. If no group was selected for an address, the columns display the same as the MAC Src. and MAC Dest. columns (instead of the group base name the address raw name will be used).
Layer 3 Src.	This column will display the layer 3 address of the system that sent a packet. This can be an IPv4, IPv6, IPX, or NSAP address. Note: Some packets will never be routed outside the LAN and therefore do not have layer 3 addresses (e.g. ARP).
Layer 3 Dest.	This column will display the layer 3 address of the system that shall receive a packet.
Layer 3 Grp. Src./Dest.	These columns will display the address group to which a layer 3 address belongs. If no group was selected for an address, the columns display the same as the Layer 3 Src. and Layer 3 Dest. columns (instead of the group base name the address raw name will be used).
VLAN ID	This column displays the ID or user defined name of the VLAN to which a packet belongs.
VLAN Grp.	This column will display the address group to which a VLAN ID belongs. If no group was selected for a VLAN ID, the column displays the same as the VLAN ID column (instead of the group base name the VLAN ID in raw format will be used).



5.7 Statistics Modules

Statistics modules are used by the Statistics View, the Load over Time Statistics View, and for report generation. They can be selected on the respective settings pages (Statistics Settings, Load over Time Statistics Settings, and Report Data) in the Settings dialog.

The statistics modules are assigned to seven different groups:

A) Network Interface Statistics

This group contains only one statistics module that will display the total traffic for each network card or virtual network interface (some DSL drivers use this) of the local system.

B) Address Statistics

This group contains modules that can display the total, received, and sent traffic for every detected LAN (MAC) address or VLAN ID (both layer 2) or Internet (layer 3) address. Use the layer 2 modules if you are only interested in the traffic inside your LAN.

C) Directed Traffic Statistics

This group contains modules that can display the traffic that was sent from one LAN (layer 2) address to another LAN address, from Internet (layer 3) to Internet address, or the traffic between two systems on layer 2 or 3. When using one of the first modules (A --> B), you will get two entries for each connection, one for traffic from A to B and one for traffic in the opposite direction.

D) Protocol Statistics

This group contains modules that will show the traffic that was generated by different protocols in your network. If the Easy Statistics Mode in the Tools menu is enabled, you will get two versions of each statistics module that handles protocols. A basic version and a detailed version. The detailed version will create more statistics entries as it further subdivides some protocols. If you capture SMB data, the basic version will always display SMB while the detailed version will create different entries for SMB-Transaction, SMB-Close, etc.

In the advanced statistics mode you get a detailed and a basic version for the layers 2 to 4 and for the upper protocols above layer 4. The difference is here too that the detailed version distinguishes between some data units of protocols as well. For example: while the basic layer 4 traffic statistics will display the traffic that was generated by the TCP protocol only, the detailed version will further subdivide this to traffic that was generated by TCP data, synch, final, and reset packets.

E) Address and Protocol Statistics

This group contains statistics modules that display the traffic that was generated by LAN (layer 2) or Internet (layer 3) addresses together with the protocols that were used. It is in general a combination of the group B and D statistics modules.

F) Connection and Protocol Statistics

This group contains statistics modules that display the traffic that was generated on a connection between two layer 2 or layer 3 systems together with the protocols that were used. You can use modules for traffic in a single direction (A --> B) that will usually create two entries per connection or modules that create only one entry per connection (A <-> B). This group is a combination of the groups C and D.

G) VLAN and Protocol Statistics

This group contains modules that display the traffic that was generated in different VLANs together with the protocols that were used. If you do not want to see normal LAN traffic (packets without VLAN ID), add also a VLAN ID filter and exclude the 'No VLAN' entry; see VLAN Filter Settings.

Some tips for choosing a statistics module (the names in the brackets are displayed if you switch of the Easy Statistics Mode):

If you just want to know the network traffic that is generated by each system in your LAN, use the LAN Traffic per System (L2 Address Statistics) module from group B. If you want to check the speed of an internet connection of a single computer, use the group A Traffic per Network Card (Network Interface Statistics) module.

If you want to know which protocols are used in your LAN, use the Traffic per Protocol (Higher Protocol Statistics) module from group D; use the Detailed (Highest Protocol) module for more or any other (in advanced statistics mode) for less details.

If you want to find a system in your LAN that generates lots of traffic using specific protocols, use the LAN Traffic (L2 Addr Higher Protocol) or Internet Traffic (L3 Addr Higher Protocol) Statistics from group E or F.

Note: Currently the statistics views and the reports will show only upper TCP and UDP protocols for which the port is known. Any traffic caused by packets that are using ports for unknown protocols will be displayed as TCP traffic. So if you want to see statistics for specific ports, you may need to add them to the tcp.ports file and assign a protocol name (see 'Modifying the configuration files' for more details).



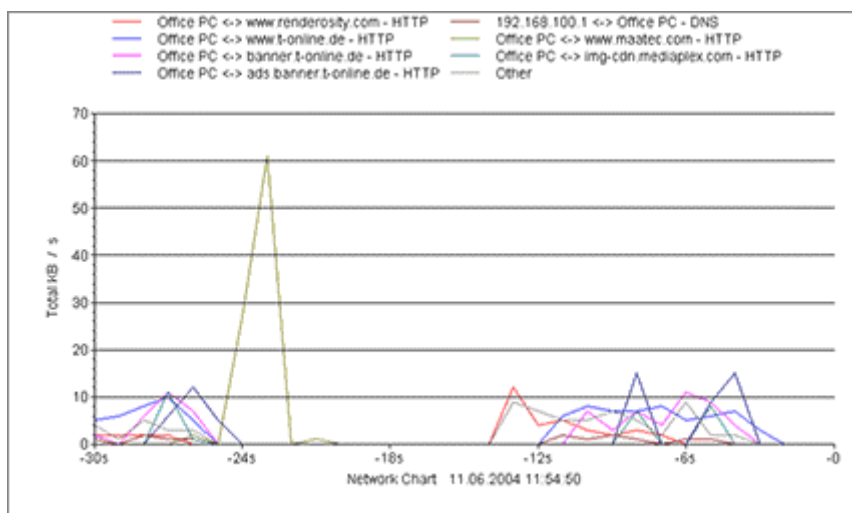
5.8 Load over Time Charts

(PRO VERSION)

You can use different chart types to display network Load over Time Statistics. Line charts can be used with large numbers of data points ('Number of values' in the settings dialog) whereas bar charts will become complex if used with more than 20-100 data points (depending on the bar chart type and screen resolution). Therefore bar charts are usually more comprehensible. Following chart types can be chosen in the Load over Time Statistics Settings dialog page:

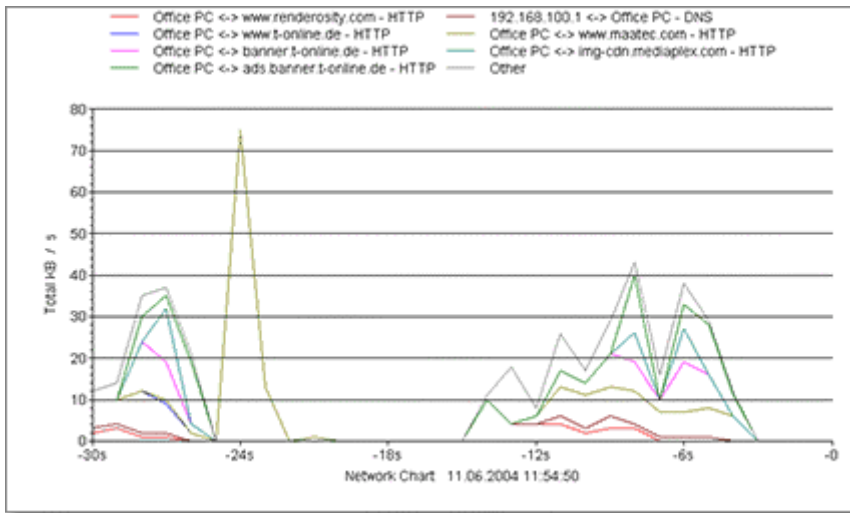
Lines

The network traffic is displayed in a simple line format. You can easily see which system or protocol caused the most traffic but it is difficult to determine the overall traffic volume.



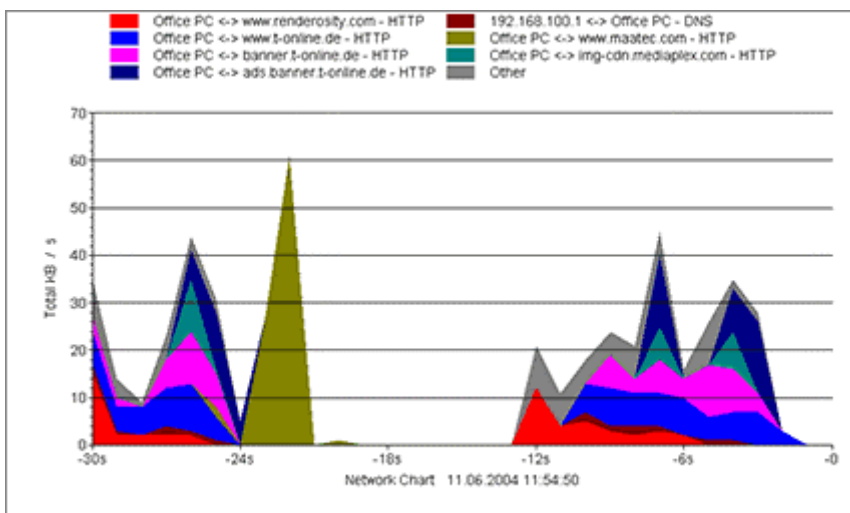
Stacked Lines

The network traffic is displayed as a cumulative set of lines - the data points are placed one upon the other. It is easy to determine the overall network traffic with this chart but the amount of traffic per single system or protocol may not be as identifiable as in the simple line chart.



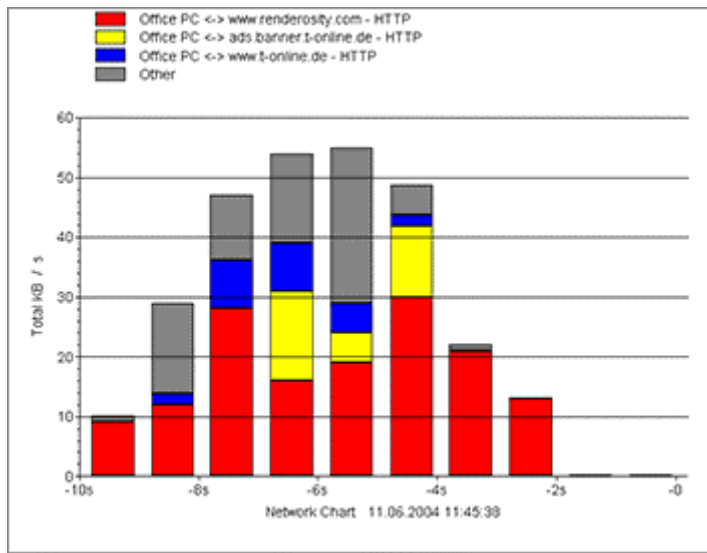
Stacked Lines Filled

This is the same chart as above but the areas between the stacked lines are filled.



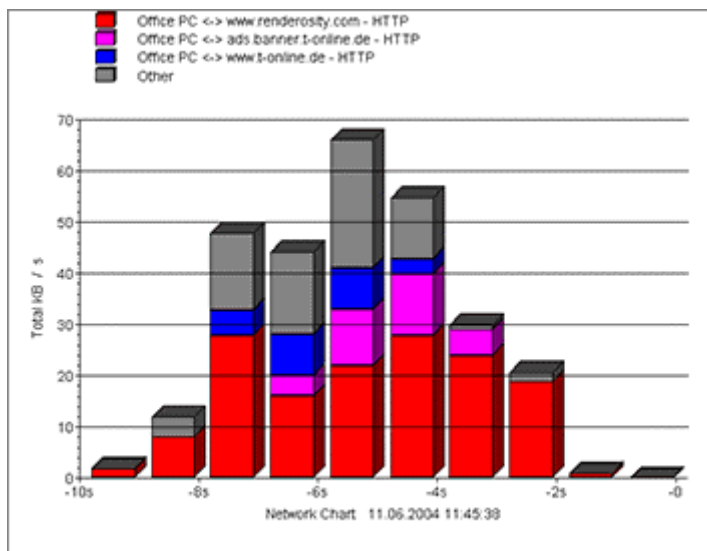
Stacked Bars

The amount of network traffic is represented by bars that are stacked one upon the other. This way you can easily determine the overall network traffic and the traffic per system or protocol. But it may be difficult to see the relation between the traffic caused by different systems. This chart type is usually well suited for up to 100 data entries.



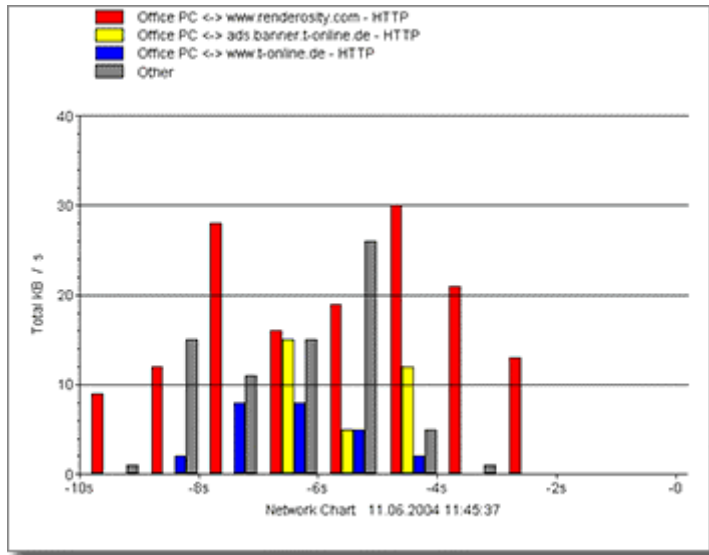
Stacked Bars 3D

Same chart as above but with 3D effect.



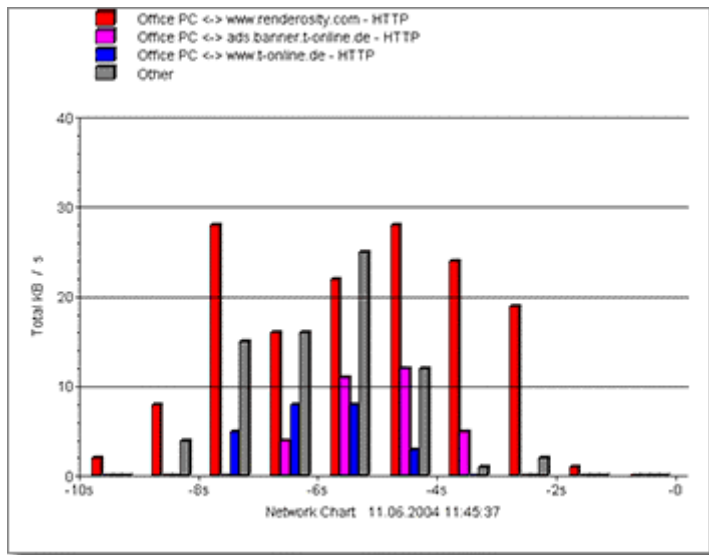
Group Bars

The network traffic per system or protocol is represented by simple bars that are placed side by side in bar groups. They allow to determine the relation between traffic volumes of different sources and to find network load peaks of single systems. But you cannot see the overall network traffic and the chart may become complex even with few 'Number of values' settings.



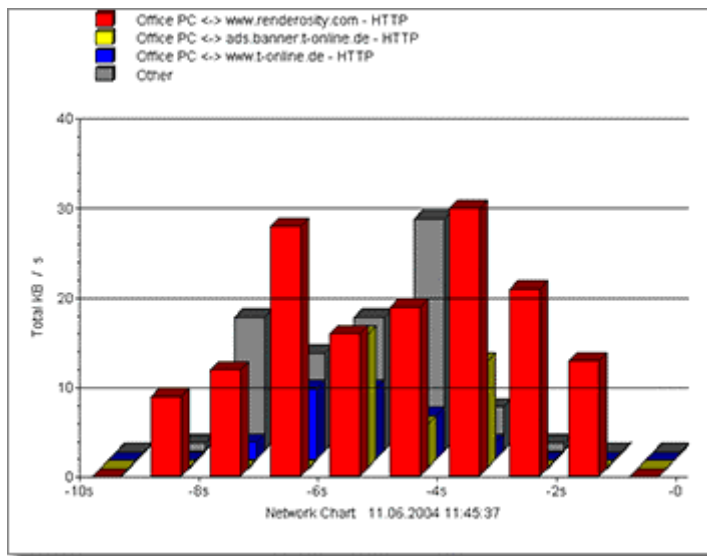
Group Bars 3D

Same chart as above but with 3D effect.



Deep Bars

Almost the same as Group Bars 3D but the bars are placed one after another and not side by side.



5.9 Report Charts

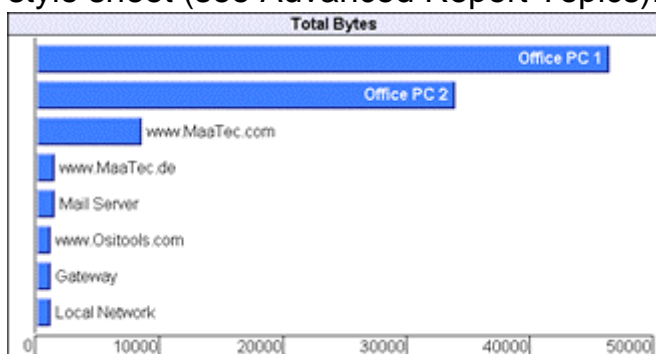
(PRO VERSION)

The Report Data page of the MTNA Settings Dialog allows to add a chart for every numeric value column of a report table. All bitmap charts are available in two sizes: Large = 640x400 pixel and Small = 320x200 pixel. The bitmap charts will be saved as transparent, compressed png files in a Chart sub-directory of the report target directory. Bitmap charts will usually add 1 to 6 KB to the report, HTML coded charts will add about 2 to 5 KB.

Currently following chart types are available:

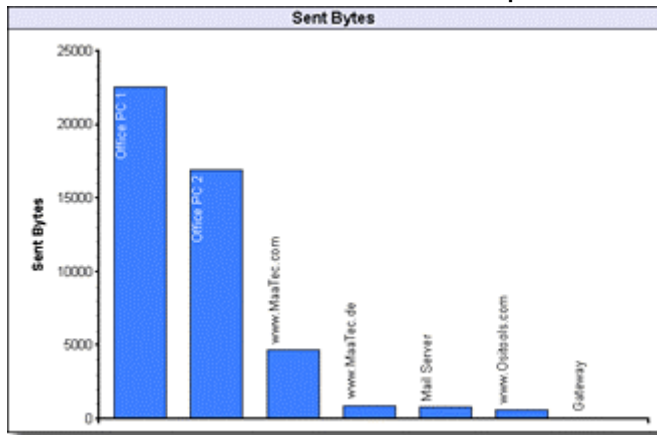
Horz Bar (HTML)

A horizontal bar chart that is generated in pure HTML code. This chart will scale itself to fit the browser window width. But due to HTML, its resolution is limited to 1% steps. You can modify the bar color and distance via the report style sheet (see Advanced Report Topics).



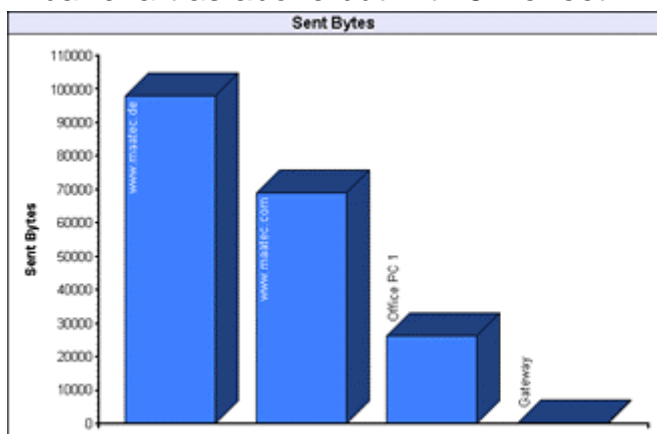
Bar

A vertical bitmap bar chart. The bars are scaled to fit the bitmap width. The labels are contained in the bitmap.



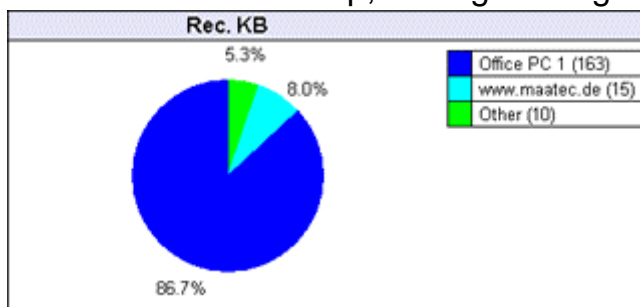
3D Bar

A bar chart as above but with 3D effect.



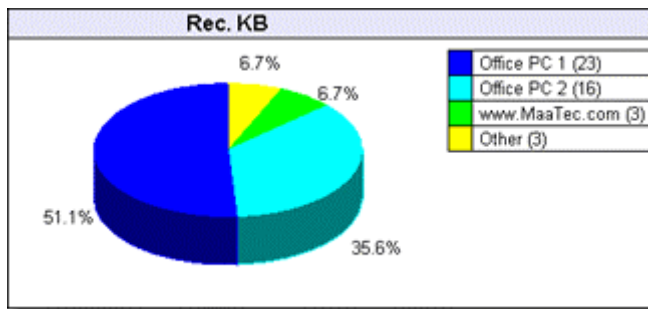
Pie

A pie chart with HTML legend. Small pie charts will not display values that represent less than 5% of the total, large bar charts will not display values less than 3%. Otherwise the labels may overlap. The percentage labels are contained in the bitmap, the legend is generated as HTML.



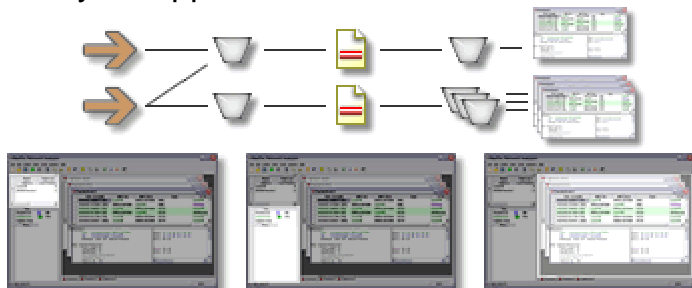
3D Pie

Same as Pie but with 3D effect.



5.10 Data Flow

This diagram demonstrates the data flow through the MaaTec Network Analyzer application:



Packet Sources (Network Cards) Packet Sinks (Documents) Packet List View

Packets are collected from the network. You choose the network interface cards (Packet Sources) to collect data from in the Settings dialog that opens when a new document is created.

Each document can collect and store data from one or more Packet Sources. The kind of packets that shall be stored in the document may be restricted by a capture filter. You can open multiple documents for collecting data with different capture filters at the same time.

The packets of each document are displayed in one or more views. Each of the views can use a view filter to display only a subset of the stored packets.

5.11 Capture Filter





A capture filter is used to restrict the kind of packets that will be stored in a document when collecting network data. In contrast to a view filter all packets not passing the capture filter are lost. So if you not feel certain about which packets to filter, you should use a view filter instead.



A capture filter is always applied when a new document is created, though it will let pass all packets by default. To change the capture filter settings for an existing document use the Collect > Capture Filter menu command. In both cases the Settings dialog for the capture filter will open. In addition to the Settings dialog for the view filter you can choose the packet sources here. These are the network interface cards that shall be used to collect packets. On the same page it is possible to change the buffer size of the packet store. But this is only possible for new documents and the control will be read only when editing capture filters of existing documents.

5.12 View Filter



A view filter is used to restrict the packets that are displayed in a document's view (e.g. Packet List View). In contrast to a capture filter the view filter does not reduce the amount of packets stored in the document. So there is no risk of losing packets when view filters are set up.

 To add or change a view filter for the current view, click the View Filter button , use the View > View Filter menu command, or press F10 on the keyboard. This will open the Settings dialog where you can modify the filter's parameters.

 To remove a view filter completely from a view, click the Remove View Filter button , use the corresponding menu command in the View menu, or press Ctrl+F10 on the keyboard.

Note: If you remove a view filter and then add one to the same view again, the settings dialog will use the address filter values of the previous filter. So you can apply the previous filter by simply clicking OK. If you want to clear these values, go the Save and Load page in the Settings dialog and click Reset All.



5.13 Address Filter

Address filters allow to reduce the number of packets stored in the document (capture filter) or displayed in views (view filter) depending on the source or destination addresses of the packets. Use the Address Filter pages of the Settings dialog to enable and modify the different address filters.

Each packet will at least have a MAC (Media Access Control) source and destination address. These are Network Layer 2 addresses that are only visible in the current LAN. (A LAN is a Local Area Network. It contains a number of computer and/or other systems, which can send data to each other system without using a router. All systems are directly connected via hubs or switches.) Most packets will also contain network layer addresses (e.g. IP addresses). These addresses are needed to exchange network data between LANs. If packets have been sent to or received from outside the LAN their Layer 3 addresses may belong to other systems than their MAC addresses. If for example a packet is received from an outside web server, the IP source address will belong to the web server while the MAC source address belongs to the gateway of your LAN that handles the traffic to and from this web server. This gives some hints on which filters to use for which purpose:

- To observe the network traffic to and from specific systems in your LAN use a MAC address filter containing the addresses of these systems.
- To observe the traffic going outside from the LAN and vice versa use a MAC address filter as well, but use the gateway's address.
- To observe traffic to and from systems outside the LAN (e.g. a specific web server) use the layer 3 address filters.

Of course you can use the layer 3 filters for filtering traffic inside your LAN, too. But to get only packets for a single system, you may need more than one filter in this case. This is because the layer 3 filters do not interact with each other and thus an IP address filter will let pass any non-IP packet like IPX or CLNP. Though, if you are not interested in these other protocols, you can use the protocol filter to remove the corresponding packets.

Note: If the computer on which the Network Analyzer is running is connected to the LAN via a switch, it will only collect packets sent from or to this computer and packets sent to multicast MAC addresses (first address byte is odd) because the switch won't forward other packets to this computer. To collect other than these packets, you have the following options: Some switches may offer a service connector to which all data is sent. Otherwise use a hub instead of the switch or install and run the Network Analyzer on all systems you need to observe.



5.14 Address Filter Examples

If a packet with source address A and destination address B is collected from the network, the following tables will show whether it passes an address filter or not depending on different filter settings.

Note: If the source or destination filter is set to Off, the Link setting is ignored and the address filter will work as if it contains only the filter which is not switched Off. So if Source is Off and Destination is set to exclude address B, all packets destined to B will be discarded independently from their source address. A filter is implicitly set to Off if its address list is empty.

Case 1: Address A is contained in the source filter list and address B in the destination filter list:

Source Incl/Excl	Link	Destination Incl/Excl	Pass
Off	Or/And	Off	Yes
Off	Or/And	Incl	Yes
Off	Or/And	Excl	No
Incl	Or/And	Off	Yes
Incl	Or	Incl	Yes
Incl	Or	Excl	Yes
Incl	And	Incl	Yes
Incl	And	Excl	No
Excl	Or/And	Off	No
Excl	Or	Incl	Yes
Excl	Or	Excl	No
Excl	And	Incl	No
Excl	And	Excl	No

Case 2: Neither address A is in the source filter list nor is address B in the destination filter list:

Source Incl/Excl	Link	Destination Incl/Excl	Pass
Off	Or/And	Off	Yes
Off	Or/And	Incl	No
Off	Or/And	Excl	Yes
Incl	Or/And	Off	No
Incl	Or	Incl	No

Incl	Or	Excl	Yes
Incl	And	Incl	No
Incl	And	Excl	No
Excl	Or/And	Off	Yes
Excl	Or	Incl	Yes
Excl	Or	Excl	Yes
Excl	And	Incl	No
Excl	And	Excl	Yes

Case 3: Address A is contained in the source filter list, but address B is not contained in the destination filter list:

Source Incl/Excl	Link	Destination Incl/Excl	Pass
Off	Or/And	Off	Yes
Off	Or/And	Incl	No
Off	Or/And	Excl	Yes
Incl	Or/And	Off	Yes
Incl	Or	Incl	Yes
Incl	Or	Excl	Yes
Incl	And	Incl	No
Incl	And	Excl	Yes
Excl	Or/And	Off	No
Excl	Or	Incl	No
Excl	Or	Excl	Yes
Excl	And	Incl	No
Excl	And	Excl	No

The last case, where A is not in the source filter list but B is contained in the destination filter list should now be an easy exercise.


5.15 Address Filter Tips



Here are some tips on how to configure the address filter for some common tasks.

Include data

- To observe traffic coming from a single computer, add its address to a source include filter and switch the destination filter off.

- To see the packets coming from and going to a single computer, add its address to the source and destination filter lists, set both to **Incl** and set the linkage to **Or**.
- To observe the traffic between two computers, add their addresses to the source and destination filter lists (double-click each or select both and click the  button), set the filters to **Incl**, and set the linkage to **And**.



Exclude data






- To exclude traffic of one or more PCs completely, add all their addresses to the source and destination filter lists (e.g. by double-clicking them in list on the left), set both filters to **Excl** and the linkage to **And**.
- To exclude data that is sent from one system to another, add the first address to the source list and the second to the destination list. Set both filters to **Excl** and set the linkage to **Or**.
- To exclude traffic between two PCs, add their addresses to the source and destination filter lists, set both filters to **Excl**, and set the linkage to **Or**.



5.16 Address Name Formats

Most dialogs and views of the Network Analyzer can display addresses in three different formats. The 'User' format will display the user-defined name of an address. This name can be modified on the Address Filter pages of the Settings dialog or in the Edit Address Information dialog. If no name was defined, the 'System' format is used instead. The following table gives an overview of the different 'System' and 'Raw' address name formats used in the Network Analyzer address database and a short description of the edit box in the corresponding address filter dialog. The edit box can be used to add addresses in the raw format to the address database.

	System Name	Raw Name	Edit
	Vendor Name + 6 hexadecimal digits (MC appended for multicast addresses)	12 hexadecimal digits	Enter exactly 12 hexadecimal digits
	Computer name as found in DNS packet	4 decimal numbers between 0 and 255 separated by dots	Enter up to 4 decimal numbers between the dots; missing numbers will be replaced with zeros

	Currently same as Raw Name	Compressed IPv6 format; 8 groups of up to 4 hexadecimal digits separated by colons; the first sequence of zero groups is replaced with a double colon	Enter up to 4 hexadecimal digits per colon separated group; missing digits will be replaced with zeros
	Currently same as Raw Name	8 hexadecimal digits for the network and 12 hexadecimal digits for the host separated by a colon	Enter up to 8 hexadecimal digits for the network before the colon and up to 12 behind it; leading zeros are automatically added
	Same as Raw Name	2-16 hexadecimal digits	Enter an even number of 2 to 16 hexadecimal digits (usually 12)
	Printable characters of the name and the last byte in hexadecimal format	32 hexadecimal digits	Enter exactly 32 hexadecimal digits
	Same as Raw Name	1 to 4 decimal digits	Enter a number between 1 and 4095 (12 bits)

5.17 Address Groups



Address groups are used to collect statistical data for groups of addresses instead of single ones (e.g. traffic per department). They are most useful in the statistics views (Statistics View, Load over Time Statistics View) and for reports. This will also reduce the number of different entries in the statistics views. In addition, the Packet List View will display address group information when MAC Grp. or Layer 3 Grp. columns are added via the Packet List Columns Settings page of the Settings dialog.

Use the Address Group Settings page to manage and create new address groups. To add addresses to an address group, open any Address Filter page in the Settings dialog, select all addresses that you want to assign to a group, and select the group with the group combo box below the address list.

If an address is not assigned to a group, the group combo box will display '<no_group>'. These addresses will be displayed with their own names in the address group statistics and columns.

You can use address groups to create department based statistics, to group sub-domains under their main domain name, or to group different IP addresses of a single domain that is hosted by multiple web-servers for load balancing.



5.18 Protocol Filter

The protocol filter allows to reduce the number of packets stored in the document (capture filter) or displayed in views (view filter) depending on the protocol, packet type or source and destination ports of the packets. Use the Protocol Filter page of the Settings dialog to enable and modify the protocol filter.

When different computer systems shall communicate over a network, there is the need to agree on a common structure for the data that is exchanged between them. For this purpose protocol descriptions are used that establish a number of data encoding rules. As different tasks in the network communication require different actions and parameters, it is often not feasible to use a single protocol for all aspects of the communication. Therefore some protocols are solely used for the data linkage between the physical components of the network and the software, others are used to address specific systems or subsystems in a local network or to route data between sub-networks. As a consequence a network packet is usually composed of interlocked data blocks, each encoded in accordance with a different protocol description. This can be considered as a stack of protocols, whereat each protocol is processed on a different layer of the network communication. This need to be taken into account when setting up a protocol filter. A packet will only pass this filter if all protocols that were used to encode this packet are activated in the filter.

Examples for TCP/IP and OSI Transport:

You will always need to activate a data link layer protocol. This is usually Ethernet (or Token Ring or FDDI). Ethernet is further subdivided into the protocols Ethernet II, Novell Ethernet, SNAP and LLC. For TCP/IP traffic you will in most cases need to activate Ethernet II, but IP data can be encoded inside any of the above protocols. For ISO OSI activate LLC and at least its LLC UI packet type.

On the network layer activate the network data and routing packets as needed. For IP this is always IP and any of IPv4 or IPv6. For ISO OSI activate ISO Network Layer, CLNP, and CLNP - Data.

On the transport layer and higher layers activate UDP and/or TCP with all needed TCP packet types and all upper layer protocols you want to see (e.g.

HTTP, DNS, POP3, etc.). For ISO OSI activate ISO Transport Layer, OSI TP, and any OSI TP packet type.

Note: It will in general be more convenient to uncheck the protocols you don't want to see than to set up the needed protocol stack from scratch.

Note: You can add the port numbers of missing TCP and UDP protocols to the MTNA configuration files. See [Modifying the configuration files](#) for more information.

6 Registration



If you want to register the MaaTec Network Analyzer, visit the MaaTec MTNA page at <http://www.maatec.com/mtna/purchase.html>, and follow the instructions on how to purchase a valid license.

You will receive a license key via email. Open the Register MTNA dialog with the Register Network Analyzer command in the Help menu. Enter the registration name that was used for licensing (your name or a company name) in the upper edit box and the license key in the edit box below. Then click the OK button.

If you get a message that your license key is invalid, make sure that you have used the correct registration name (case-sensitive!) and that there are no typing errors in the license key.

If you lost your license key, send an email with your registration information to support@MaaTec.com.

7 Index

- 3**
- 3D Bar..... 83
- 3D Pie 83
- A**
- About Box 66
- About button 66
- About Network Analyzer 72
- Add Scheduled Task..... 17
- Add/Remove button 1
- Add/Remove Programs 1
- Address Filter..... 86
- Address Filter Examples..... 87
- Address Filter Settings..... 42
- Address Filter Tips..... 89
- Address Group Settings 46
- Address Groups..... 91
- Address Name Formats..... 90
- Addresses list 9
- All Details..... 70, 73
- All Details button..... 7, 30
- Alt key 58
- Analyzing
 - Data 7
- Analyzing 7
- Appearance 62
- Application
 - Customizing..... 21
 - toolbars..... 58
 - uninstall 1
- Apply..... 9, 36
- Apply button..... 9, 36, 57, 60
- Arrange Icons 72
- Ascend.png..... 17
- Auto Scrolling..... 70, 73
- Auto Scrolling button..... 6
- Auto Scrolling menu..... 6
- Auto-Update Address DB 71
- B**
- B/W 9, 30, 31, 70
- Bitmap..... 83
- Bookmarks..... 7
- Border 63
- Buffer Settings 38
- Buffer size..... 6
- Button Appearance..... 58
- C**
- Capture Filter 36, 85
- Capture Filter menu 9, 85
- Charts 4, 17, 55, 78, 83
- Collect
 - Packets..... 6
 - use..... 6, 9, 85
- Collect..... 6, 9, 36, 85
- Collecting Packets 6
- Color
 - IP 40
 - List View 19
 - Time/Length 19, 38, 65
- Color 19, 38, 40, 65
- Color Selector 65
- Command line..... 17
- Commands list 60
- Common Details 70, 73
- Common Details button 7, 30
- Compressed IPv6 90
- Configure 6
- Conflict..... 60
- Context-sensitive 25
- Copy 9, 65
- Copy menu 9
- CPU 23
- Create New button..... 39
- Ctrl key..... 7, 28, 58
- Ctrl+C..... 9
- Ctrl+F 69
- Ctrl+F10 9, 28, 70, 86
- Ctrl+F2 7
- Ctrl+F4 11, 67
- Ctrl+F8 6
- Ctrl+N..... 6, 28, 67

MaaTec Network Analyzer

Ctrl+O	11, 28, 67	Excl	9, 42, 87
Ctrl+P	9, 68	Exclude	42
Ctrl+S	11, 67	Existing	
Ctrl+Shift+Tab	12	toolbars	63
Ctrl+Tab	12, 72	Existing	63
Ctrl+X	60	Expiry	66
Customize		Export	39, 68
Application	21	Export Address DB	68
Customize	12, 21, 57	F	
Customize Commands	58	F1	25
Customize dialog		F10	9, 28, 70, 86
open	21	F2	7, 27, 39, 40, 42
use	57	F3	69
Customize dialog	12, 21, 57	F8	6
Customize menu	12, 21	FDDI	92
Customize Shortkeys	60	File menu	28, 36, 39, 64
Customize Tabbed MDI	62	File Open dialog	68
Customize toolbars	63	File Properties	64
D		Filter	23
Data		Find Next	69
Analyzing	7	Finding	
Data	7, 92	Text	69
Data Flow	85	Finding	69
Decode View	30	Fonts	19, 59
Descend.png	17	H	
Destination	42, 87	Help	
Destination Incl/Excl	87	use	25, 65, 66
Detail	7, 30	Help	25, 65, 66
Detail submenu	7, 30	Help button	
Display		Clicking	25
File Open dialog	68	Help button	25, 36, 57
MTNA	72	Help Menu	72, 94
Network Analyzer	72	Help Topics	25, 72
Display	62, 68, 72	Hex View	31
DLLs	40	Horz Bar	83
DNS	40, 90, 92	HTML	17, 53, 83
Document	6, 74	HTML reports	17, 53
Drag	40, 58	I	
E		Icons	58
Edit Address Information Dialog ..	64	Import	39, 68
Edit Menu	69	Import Address DB	68
Empty Buffer	6, 73	Incl	9, 42, 87, 89
Ethernet	40, 92	Including	39, 40, 42

- Insert..... 27, 39, 40, 42
- Install
 - Network Analyzer 1, 2
- Install 1, 2
- Installation Guide 1
- IP
 - color..... 40
- IP 19, 40, 86, 92
- IPv4..... 40, 92
- IPv6..... 40, 92
- IPX 22, 40, 86
- Ipx.sockets..... 22
- L**
- L3 Dest 28
- L3 Src 28
- LAN..... 28, 86
- Layer 28, 86
- Link 87
- List View
 - Coloring 19
- List View 19
- LLC 92
- Load button..... 39
- Load Filter Settings..... 36, 39
- Load over Time..... 4, 34, 52, 78
- Load Page 23, 36, 39
- Loading 23, 86
- Loading Data 11
- Local Area Network 86
- Lost Packets 23
- M**
- MaaTec..... 2, 94
- MaaTec MTNA..... 94
- MAC
 - contains 38
 - names..... 22
 - open 9
 - use..... 86
- MAC 9, 22, 27, 28, 38, 86
- MAC Address Filter..... 42
- MAC Dest 9, 28
- MAC Src 9, 28
- Main Window 11, 26
- Main Window Overview 12
- MC 90
- Media Access Control..... 86
- Menus 69, 70, 71, 72
- Minimum Details 70, 73
- Minimum Details button 7, 30
- Modify 17, 21, 58
- More Help 25
- MTNA
 - Displays 72
 - open 25
 - Starting 2
 - use..... 1
- MTNA..... 1, 2, 7, 25, 72, 92
- Mtna.css file..... 17
- Mtna.exe file
 - run 1
- Mtna.exe file 1
- Multicast..... 90
- Multicast MAC..... 86
- N**
- Names
 - MAC 22
- Names 22
- Network Analyzer GUI 71
- Network Analyzer Main Window.. 12
- Network Cards 85
- Network interface cards..... 6, 85
- Network Layer..... 86
- Network Load..... 4, 34, 78
- New button..... 6, 28
- New menu..... 6, 28
- New Menu item..... 58
- New Toolbar button 63
- New toolbars..... 12, 63
- New Window..... 11, 72
- Next/preceding..... 7, 28
- NIC..... 21, 27, 28, 38
- Novell Ethernet 92
- O**
- Open
 - About Box..... 66
 - Customize dialog..... 21

MaaTec Network Analyzer

Edit Address Information dialog	64
Register MTNA dialog	65
Save As dialog	67
Search dialog	69
Settings dialog.....	9
Windows.....	11
Open ...	9, 11, 21, 25, 64, 65, 66, 67, 69
Or/And	87
Orientation	62
Overwrite button	39
P	
Packet Filtering	9
Packet List Toolbar	73
Packet List View	28, 40, 85
Packet Loss	23
Packet Sink View	28
Packet Sinks	85
Packet Source View.....	27
Packet Sources.....	38, 85
Packet Sources list	38
Packet Sources Window.....	26
Packets	
Collecting.....	6
Packets	6
Page Down	7, 28
Page Up.....	7, 28
Pie.....	83
Png	83
Print	68
Print button	
clicking.....	9, 31
use.....	30
Print button	9, 30, 31
Print Preview.....	9, 68
Print Setup	68
Properties	19, 64
Protocol Filter.....	92
Protocol Filter Settings.....	40
Protocol Groups	
modify	21
Protocol Groups.....	9, 21
Protocol Type Filter Settings.....	40

Q	
Quick Load.....	39
Quick Load list	
changes.....	36
use.....	39
Quick Load list	21, 23, 36, 39
Quickstart.....	6, 72
R	
Raw Name	90
Register	65, 94
Register MTNA Dialog	
open	65
Register MTNA Dialog.....	65, 94
Register Network Analyzer	72, 94
Registration.....	94
Remove View Filter.....	70, 73
Remove View Filter button.	9, 28, 86
Remove/repair dialog.....	1
Reports	15, 17, 35, 53, 55, 83
Reset	63
Reset All	9, 63, 86
Reset All button	39, 60
Run	1, 2
S	
Save.....	36, 39, 86
Save All.....	11, 67
Save As	67
Save As dialog.....	67
Save button.....	11
Save Filtered.....	11, 67
Save Page	
use.....	23
Save Page	23, 36, 39
Save Selected.....	11, 67
Scheduled Tasks	17
Search dialog	
open	69
Search dialog.....	69
Separator item	
Drag.....	58
Separator item	58
Service Pack.....	1
Settings.....	23

- Settings dialog .. 6, 9, 19, 21, 23, 36, 39, 85, 86
- Setup.exe..... 1
- Shift+Ctrl+Tab..... 72
- Shift+F2 7
- Show
 - toolbars..... 70
- Show..... 58, 70
- Show Gripper..... 63
- Show Tooltips 63
- Source 42, 87
- Source Filter list..... 9
- Source Incl/Excl..... 87
- Standard Toolbar..... 73
- Start Collect 73
- Statistics 2, 17, 33, 50, 76
- Stop 6
- Stop Collect 73
- Storing
 - collected packets..... 6
- Storing 6
- Stretch 62
- Style sheet..... 17, 83
- Support Tabbed MDI 62
- Synchronization 7
- System Name 90
- System Performance 23
- T**
- Tab Control Settings..... 62
- Task Scheduler..... 17
- TCP
 - including 40
- TCP..... 19, 21, 22, 40, 92
- Tcp.ports..... 22
- Text
 - Finding..... 69
- Text..... 69
- Text Color 27, 65
- Time/Length
 - color..... 19, 38, 65
- Time/Length.... 7, 19, 23, 27, 28, 38, 65
- Toggle B/W 9, 30, 31, 73
- Token Ring 92
- Toolbar button..... 58
- Toolbars
 - application 58
 - existing 63
 - show 70
- Toolbars.. 12, 21, 57, 58, 63, 70, 71, 72
- Toolbars list 63
- Tools 12, 21
- Tools Menu 57, 71
- Tooltips 63
- Total Lost..... 23
- U**
- UDP 22, 40, 92
- Udp.ports 22
- Uncompressing..... 11
- Uninstall 1
- Uninstalling 1
- Unregister 1
- V**
- Vendor Name..... 90
- Vendor.Codes..... 22
- View .. 6, 7, 9, 26, 27, 28, 30, 31, 36, 74, 86
- View Filter 70, 73, 86
- View Filter button..... 9, 28, 36, 86
- View menu 12, 70, 86
- W**
- Window menu 12
- Windows 1, 11, 23, 65, 67, 74
- Windows 2000 2
- Windows 2003 2
- Windows 98 2
- Windows Explorer..... 2
- Windows Installer..... 1
- Windows NT 1, 2
- Windows XP 2
- X**
- XHTML..... 17, 53