

KerioNetworkMonitor2™

User's Guide

Kerio Technologies

© 2001-2003 Kerio Technologies. All rights reserved.

Printing date: April 10, 2003

Current product version: *Kerio Network Monitor 2.1.0*. All additional modifications and up-dates reserved.

Contents

- 1 Introduction 5**
- 2 Quick Checklist 7**
- 3 Technical Information 9**
 - 3.1 *Kerio Network Monitor* Components 9
 - 3.2 How does *Kerio Network Monitor* work? 9
 - 3.3 Technical Limitations 12
- 4 Installation 15**
 - 4.1 Upgrade and Uninstallation 16
 - 4.2 Importing the License Key 16
- 5 Program Control 19**
 - 5.1 Logging in the Viewer 19
 - 5.2 Controlling the Service 20
 - 5.3 Initial Configuration 21
- 6 Configuration 23**
 - 6.1 IP Addresses Ranges 23
 - 6.2 Monitored Services 27
 - 6.3 User Accounts 29
 - 6.4 Log Settings 32
 - 6.5 Protocol Monitoring Parameters 34
 - 6.6 WWW Interface Parameters 35
 - 6.7 Additional Settings 37
- 7 Viewing and Analysis of Captured Data 41**
 - 7.1 List of Computers 42
 - 7.2 Traffic chart 45
 - 7.3 Current Connections 46
 - 7.4 Tree of Scanned Data 49
 - 7.5 Status Information 51
 - 7.6 Transferred Data Volume Table 53
 - 7.7 Log Windows 55

8	Web Interface	59
8.1	Connection to the Web Interface	59
8.2	Page <i>Main</i>	60
8.3	Page <i>Chart</i>	60
8.4	Page <i>Report</i>	60
8.5	Page <i>Connections</i>	61
8.6	Page <i>Logs</i>	61
8.7	Integration of the WWW Interface into the Company Website	61
9	Glossary of Terms	67
10	Index	69

Chapter 1

Introduction

Kerio Network Monitor is a small, though powerful tool for online monitoring of network traffic. It offers a whole set of choices which activities and events can be monitored.

Line load chart The online display of the Internet connection load (incoming and outgoing traffic) in the time range from 1 minute and 1 year. The average transfer speeds are shown for 3 seconds (1 minute graph) up to for 3 days intervals (for 1 year graph). Both the total traffic and the traffic for particular users (workstations in the network) can be displayed at once. This way, you can quickly find out the workstation generating the biggest load on the Internet connection.

By default, the traffic for all available services (e.g. WWW, FTP, TELNET etc.) is displayed. Besides, the traffic for particular services (predefined or custom — determined by a protocol and a port number) can be displayed and their traffic can be watched separately. The traffic is shown for particular IP addresses which can be translated into the names of computers (taken from DNS or entered manually).

Total volume of data within a given time period From acquired data you can identify, who in your network uses the Internet in the most intensive way. It is possible to create statistics with a day, week or month increments (e.g. the last 2 months with week increments for all or only some selected computers).

Current connections It is possible to watch a in special window in (almost) real time, which connections have the particular stations opened. The history of those connections is recorded in the (*Connection Log*).

Tree of captured data *Kerio Network Monitor* is able to store detail data of certain protocols (e.g. SMTP, POP3, IMAP, HTTP, etc.). The data is displayed as a neat tree, where it can be sorted according to the stations (IP addresses) or the protocols. Optionally, it is possible to store also the content of the sent E-mail and the visited WWW pages (if they are not transferred using encrypted protocols).

Log of visited WWW pages The *HTTP Log* window records all the captured HTTP requests. The selection of a computer from the list is differentiated by color all request generated by this particular station.

E-mail log Window *Mail Log* stores information about all E-mail messages; both sent via the SMTP protocol, as well as downloaded via the POP3 or the IMAP (if they were not

Chapter 1 Introduction

transferred using encrypted connections). The sender address, the recipient address and the size of sent message are stored.

ICQ log Use the *ICQ Log* dialog to view information on communication through *ICQ* and *ICQ2Go* protocols. ICQ numbers and nicknames of senders and recipients as well as message body are logged.

Remote access *Kerio Network Monitor* has separated monitoring service (*Daemon*) and the user interface. These two components communicate together via the TCP/IP protocol. It results in the possibility of watching and configuration not only locally but also remotely from any other computer.

WWW access *Kerio Network Monitor* contains embedded WWW server, which enables viewing and evaluation of the data using a standard WWW browser. It offers major part of the functions, which are included in the user interface (with exception of the program configuration).

User accounts When connecting to the service, user name and password are required. Therefore more users can be connected simultaneously to *Kerio Network Monitor* with different levels of the access rights (viewing, configuration, administration of the user accounts, ...).

Export of data The data created by *Kerio Network Monitor* is possible to be further processed: the chart can be stored as an image, the statistics for particular time frame can be stored into the CSV format (can be processed by e.g. Microsoft Excel), the logs can be processed by an external analyzer (e.g. *Kerio Log Analyzer*).

How can you use Kerio Network Monitor?

- you want to have an overview how individual computers in your firm put load on the Internet line
- you need a basis for charging particular users (computers) for the costs of the Internet connection.
- you require an audit of your employees' Internet browsing
- you are interested in which WWW pages they visit, which files they download, who they send E-mail to...
- searching for and finding the solutions to your problems — *Kerio Network Monitor* offers you a lot of information about the history of the communication in your network.

Chapter 2

Quick Checklist

This chapter gives you a basic step-by-step guide to quickly set up the important parameters of *Kerio Network Monitor* program so that it can be used immediately. If you are unsure about any of its steps, look up the chapter dealing with the appropriate problems.

1. Choose suitable computer in your network and install both components of *Kerio Network Monitor* on it (see chapters 4 and 3.3).
2. Log in to the viewer (see chapter 5.1) and choose the adapters, on which the packets are to be monitored (see chapter 5.3).
3. In the menu *Action / Change password* set the password for user Admin.
4. If no private IP addresses are used in the local network set appropriate ranges of IP addresses in the menu *Settings / Configuration*, the *IP addresses* tab (see chapter 6.1).
5. If the local network is connected to the Internet via a proxy server, check and, if necessary, adjust the settings for the proxy server in the menu *Settings / Configuration*, the *IP addresses* tab (see chapter 6.1).
6. If an mail server is running in the local network or on the internet gateway, decide how the amount of transferred mail should be measured and perform the appropriate settings the in menu *Settings / Configuration*, the *IP addresses* tab (see chapters 3.3 and 6.1).

Chapter 2 Quick Checklist

Technical Information

3.1 *Kerio Network Monitor* Components

Kerio Network Monitor consists of two separate components:

Watching service (*Daemon*) The executive core of the program that captures the packets and saves the data into a file on the disk. It runs as a service (in Windows NT/2000/XP) or as a background application (in Windows 9x/Me).

Viewer It is intended for viewing and analyzing gathered data and configuration of the service. The communication between the viewer and the *Daemon* is kept using the protocols of the TCP/IP standard — thanks to this fact it is possible to connect not only from local (from the same computer) but also from any other computer in the local network respectively in the Internet. The detail description is located in chapter 5.1.

3.2 How does *Kerio Network Monitor* work?

Packet Monitoring

Kerio Network Monitor Daemon watches the network traffic in so called promiscuous mode (i.e. it can accept also the data that is not addressed to the computer on which it is running). It captures all the IP protocol packets from which it extracts the required information:

Volume of transferred data In each captured IP packet test of the source and the target address is performed. If one of these addresses belongs to the local network and the other to the Internet (it deals with transfer between the local network and the Internet), the size of the data part of transport protocol (TCP or UDP) is measured and this figure is stored. In case that both addresses belong to the local network or to the Internet, size of the data is not stored.

Program configuration defines if the IP addresses belong to the local network or to the Internet — see chapter 6.1.

Note: Various network monitoring tools use different methods for measuring of the volume of transferred data (e.g. whole Ethernet frames, size of the data in IP packets

Chapter 3 Technical Information

including headers, etc.). The information gathered by *Kerio Network Monitor* can therefore differ from those acquired by the other tools (the deviation should not exceed 40% — if there is several times higher difference, it is necessary to look for the mistake in the network or in the program configuration).

Viewing current connections All captured IP packets are scanned for TCP segments opening and closing connection (with attributes *SYN* and *FIN*). So *Kerio Network Monitor* has information about all open connections of individual workstations in the network. In similar way information about communication via UDP protocol is displayed. Because it is datagram-oriented protocol so called pseudo-connections are evaluated — connection lasts until interval of UDP datagram exchange between source and target station exceed predefined time (default: 180 seconds).

Monitoring of services Each of the captured IP packets is checked if it contains data from some of the defined services (see chapter 6.2). In positive case the data is stored. As an example, we present the transfer of E-mail via the SMTP protocol. If the TCP connection with the target port 25 is recorded, all packets belonging to this connection are monitored and from them E-mail address of the sender and the recipient of the message, eventually the content of the message can be reconstructed.

Configuration File

Kerio Network Monitor configuration information is stored in the `NetMon2.cfg` file. This file is saved under the directory where *Kerio Network Monitor* is installed (typically `C:\Program Files\Kerio\Network Monitor`). Simply copy this file to backup your settings.

Warning: Stop *Kerio Network Monitor Daemon* before taking any action with the configuration file (refer to chapter 5.2)!

Data Storage

The measured data is stored in binary files on the disk. In the data folder (by default the same, where *Kerio Network Monitor* is installed), the following subfolders are created:

- `high` — data with high resolution (sampling rate 3 seconds)
- `low` — data with low resolution (sampling rate 1 hour)

In these folders are created another subfolders according to the IP addresses of individual computers in the local network and in them are stored the files with the acquired

3.2 How does *Kerio Network Monitor* work?

data (the high resolution data — one file per day, the low resolution data — one file per 28 days).

Then there are created the following subfolders:

- **browse** — the information about the captured objects of the monitored services (URLs of web pages, E-mail addresses, FTP relations, etc.)
- **captured** — captured objects (e.g. captured WWW pages, E-mail messages, etc.)
- **logs** — files with the logs (see chapter 7.7)
- **debug** — the data stored for detail monitoring of particular service (see chapter 6.2)

The folder structure for storing the data is rather flexible because it enables e.g.

- merging of the data with other data (if it deals with two mutually exclusive time periods)
- deleting the logs for a particular computer (IP address)
- deleting the data of a particular service (e.g. WWW).

Before performing operations of this type, it is necessary to stop *Kerio Network Monitor Daemon* (see chapter 5.2).

Data Storage Folder Modification

In case you need to change the folder for storing the measured and captured data and the log files (so that they are for example stored to the different disk), it is possible to carry it out by modifying appropriate parameter in the configuration file.

First of all it is necessary to stop the *Network Monitor Daemon* service (see chapter 5.2). Then open in any editor (e.g. *Notepad*) the file *NetMon2.cfg* (the *Configuration File* section). The data folder is written in the `main_dir` parameter. For technical reasons the backslashes must be doubled in the path name — the path to the chosen data folder can look like this:

```
main_dir = "d:\\netmon_data"
```

The change of the data folder is best to perform immediately after the *Kerio Network Monitor* program installation, when there are not yet any measured real data. If you are changing the folder after some time of using the program, it is necessary to copy (respectively move) to the new location the folders with the acquired data and the logs, i.e. `browse`, `captured`, `debug`, `high`, `logs`, `low` a `www`.

Chapter 3 Technical Information

Warning: Subfolder `License` must remain in the same folder as the program files (i.e. where was *Kerio Network Monitor* originally installed)!

After changing the folder and possible copying the measured data you can again run *Network Monitor Daemon*.

3.3 Technical Limitations

The principle how *Kerio Network Monitor* works implies some small limitations. They are to be kept in mind especially when choosing the computer for installation of *Kerio Network Monitor*

Network Components and Network Topology

If your network contains switch (switching hub), keep in mind that it does not send all the data to all its ports! But *Kerio Network Monitor* requires all the data to be present in the segment, which is “his” computer connected to.

There are several solutions:

- install *Kerio Network Monitor* directly on the computer, which is connected to the Internet. This solution is recommended always when on the internet gateway runs Windows type operating system. (*Kerio Network Monitor* then must be set up for monitoring on the “inner” network adapters — see chapter 6.1).
- some types of switches can be configured so that they send all data to one (so called monitoring) port. The station, which *Kerio Network Monitor Daemon* runs on, can be connected to this port.
- insert small hub between the switch and the internet gateway (3 ports are enough — one for the switch, the second for the internet gateway and the third to the computer, where *Kerio Network Monitor Daemon* runs).

If the network is divided by the router to more IP segments *Kerio Network Monitor Daemon* must be installed on computer in the same segment as the internet gateway.

If the network has more segments and each of them is connected directly to the internet gateway *Kerio Network Monitor* must be installed directly on the gateway. In the other case it will monitor only the data in the segment which it is connected to.

E-mail

The natural requirement of the network administrator is also to monitor the volume of the data transferred via electronic mail (E-mail) and accepted by the local mail server.

3.3 Technical Limitations

The most common case is the situation when the mail server runs on the computer that is also the internet gateway. *Kerio Network Monitor* then “sees” only the local communication of the clients with the mail server. In the default configuration of *Kerio Network Monitor* are created rules, which consider this communication to be the Internet communication (so that the volume of the data is measured). It is necessary to keep in mind that the volume of the data is measured also when the users are sending mail locally to each other.

If the mail server runs on another (“inner”) computer, *Kerio Network Monitor* records E-mail communication outside of the local network twice: when the client communicates with the mail server in the Internet. Then it is useful to change predefined rules for the SMTP, POP3 and IMAP services so that the rules are valid only for IP address of the mail server — e.g.:

```
<192.168.1.10> <255.255.255.255> TCP25 on Internet
```

and add the rules for ignoring any other mail communication — e.g.:

```
<all addresses> <all addresses> TCP25 discard packet
```

These rules must be in the list of the rules lower than the rules for particular mail server. Detail description can be found in chapter 6.1

Proxy Server

Similarly as in the case of the mail server located on the computer, which is the internet gateway, raises the problem with monitoring the communication of the clients with the proxy server, when the data is taken from its cache — also this data will be evaluated as downloaded from the Internet.

This problem can be avoided only by switching of the cache, which can be unpleasant under some conditions.

Encrypted Connection

Data encrypted by any protocol cannot be analyzed by *Kerio Network Monitor*. Only size of transferred data can be monitored in such cases.

Chapter 4

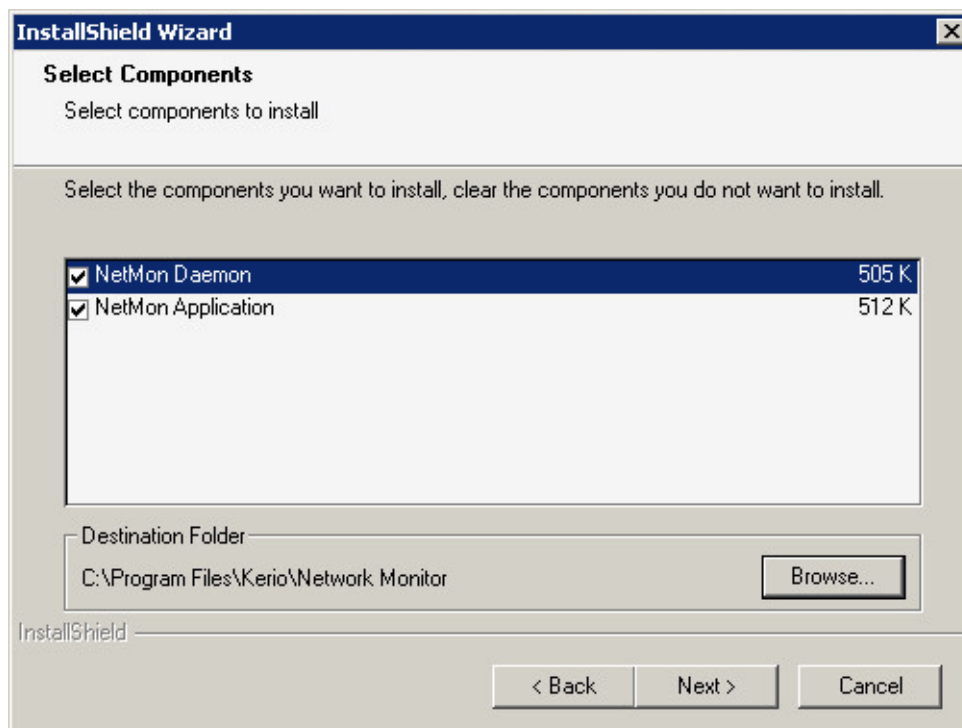
Installation

Kerio Network Monitor can be installed on any computer in your local network running Windows 95 OSR2, 98, Me, NT 4.0, 2000 or XP operating system. Older versions are not supported.

Installation is performed by running the installation archive e.g.:

```
kerio-netmon-2.10-en-win.exe
```

During the installation, the user can choose, which components of *Kerio Network Monitor* are to be installed:



NetMon Daemon Monitoring service (*Daemon*). It must be installed on the computer, where you want to monitor the communication (typically e.g. on the Internet gateway).

Note: License conditions allow to install the monitoring service only on one computer. If you want perform monitoring in more places, appropriate number of *Kerio Network Monitor* licenses must be purchased.

Chapter 4 Installation

NetMon Application Viewer. It can be installed on any number of computers, where you will connect to the service from.

Note: We recommend to install the viewer also on the computer, where will be the monitoring service (*Daemon*) installed (to allow local connection in case of any problems with the network; in the case of Windows 9x/Me it is the only way how to stop and start the service — see chapter 5.2).

The *Daemon* is started automatically (there is no need to restart the computer) after installation. From now on it is possible to log in to the viewer (see chapter 5.1).

4.1 Upgrade and Uninstallation

If you would like to upgrade *Kerio Network Monitor* or uninstall the program, you must stop the viewer. *Kerio Network Monitor Daemon* does not have to be stopped manually, because the installation program will stop it automatically.

To perform the upgrade procedure run the installation program (can be obtained e.g. from the Internet pages of its producer — www.kerio.com). The original version needn't to be uninstalled. The installation program automatically detects the folder of previous version and installs in it. After successful upgrade the *Kerio Network Monitor Daemon* is started automatically.

Uninstallation of *Kerio Network Monitor* can be performed by choosing the *Add / Remove Software* option in the *Control Panels*. When uninstalling, the folders and files within, in which the scanned data is stored, are not deleted. They must be removed manually (or can be used for the next installation of *Kerio Network Monitor*, moved to another computer, etc.).

Note: If you will forget to stop the viewer or the installation program will be unable to stop the service, the installation program will require reboot of the computer.

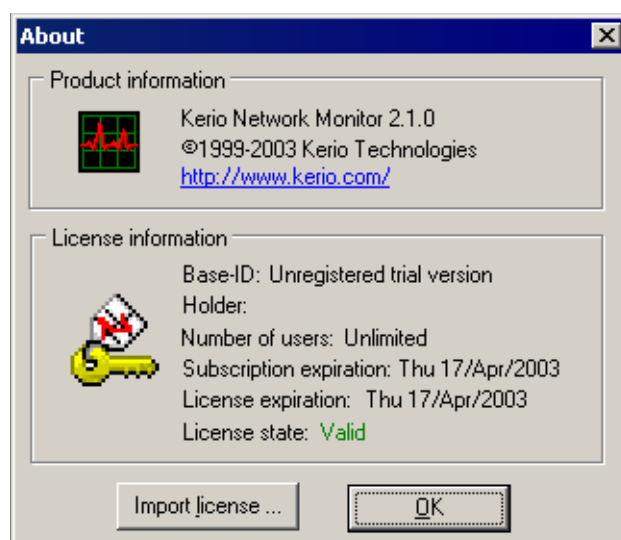
4.2 Importing the License Key

Kerio Network Monitor behaves after installation as fully functional demo version with time limitation to 15 days from the installation day. On expiration of the time, the program will stop collecting the data.

On purchase of the product, you will receive the license key — file with the digital certificate `license.key`. By importing the key, *Kerio Network Monitor* becomes full version instead of demo version, and the program can be used on for unlimited time. This procedure can be preformed also after the 15 day trial period has expired and the program is not functional. After importing the valid license key, it will work again in full extent.

Import of the license key is performed in the menu *About / About*.

4.2 Importing the License Key



Pressing the button *Import license* displays a dialog for opening the file with the license (*license.key*). When it is loaded successfully, the information about current license will appear in the section *License information*:

ID Identifier of the license (serves e.g. for verification of the license authenticity)

Holder Holder of the license — individual or organization, which bought the product.

Number of users The number of users (i.e. IP addresses of the computers in the local network, which will be monitored). If this number is reached the next IP addresses are not monitored and on the start of the viewer a warning, saying that the maximum number of users was reached, is displayed.

Subscription expiration Free program upgrade expiration date.

License expiration License validity expiration date (applicable for demo versions and time restricted version)

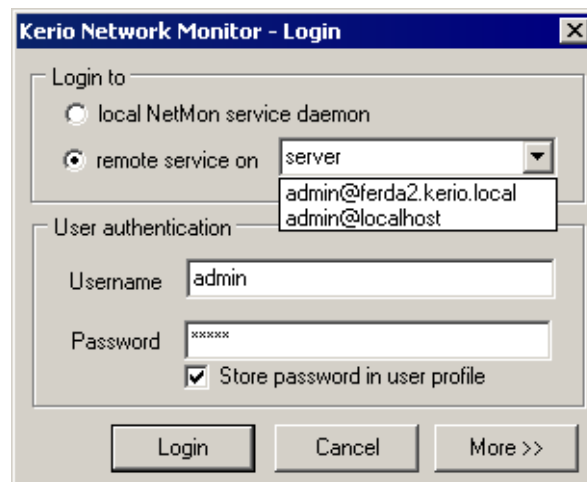
License state License state: *Valid* or *Invalid*. License is invalid if the date of its expiration occurred or the license file was corrupted, etc.

Note: If the license is invalid *Kerio Network Monitor* does not measure any data. It is still possible to log in the viewer and browse older data (measured in the time, when the license was valid), or perform configuration tasks. By importing a valid license (see above), the program functions will be restored in full extent.

Program Control

5.1 Logging in the Viewer

The viewer can be started by choosing *Programs* → *Kerio* → *Network Monitor* in the menu *Start*. The login dialog is shown after the program is started .



In the section *Login to* choose, where the *Kerio Network Monitor Daemon* service is running:

local NetMon service Daemon The service is running on the same computer as the viewer.

remote service on The service is running on another (remote) computer.

Insert IP address or DNS name of the host on which the service is running (the term “server” will be used in the further text), or select any server to which *Kerio Network Monitor* has been already connected. *Kerio Network Monitor* keeps names (or IP addresses) of all servers to which it has been connected successfully, including their usernames. Failed connection attempts are not kept. Passwords are not stored for security reasons.

Note: By entering the name `localhost` or the loopback address `127.0.0.1`, you will get the same effect as by choosing *local NetMon service Daemon* — connection to the service running on the local computer.

Chapter 5 Program Control

User authentication — enter your user name and password. In case you are logging to *Kerio Network Monitor* for the first time (after installation), use the predefined user account *Admin* and leave the password empty. To store passwords in user profiles so that it is not necessary to specify them for each connection use the *Store password in user profile* option.

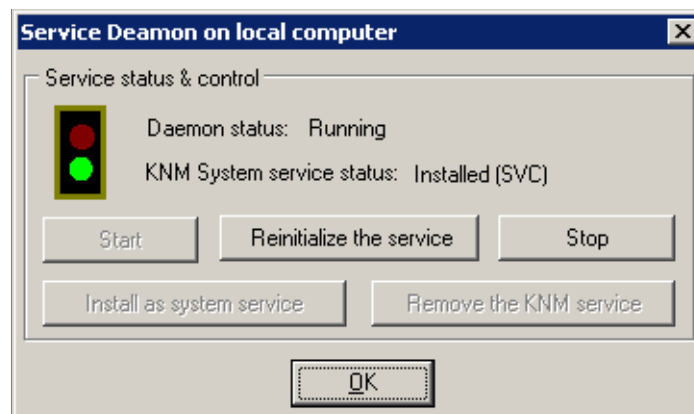
You can perform the login by pressing the button *Login*. The button *Cancel* cancels the login dialog and also closes the viewer. The *More >>* button expands the dialog by other options. When pressed, it changes to *Less <<* — it allows the expanded options to be hidden.

Store password in user profile User name and password will be stored into the user profile in Windows and it will not be necessary to enter it on each login. We recommend to use this option only when there is no risk of access rights misuse by another person!

Don't restore windows settings The viewer will not restore the layout of the individual windows. This can be helpful e.g. when connecting remotely via slow line(it can significantly decrease the amount of transferred data), or in case that more people uses the same user account.

5.2 Controlling the Service

After pressing the *More >>* button in the login dialog, the icon for configuration of the service will appear in the lower right corner of the window. On clicking it, the following dialog will appear:



Daemon status Display the status of the service — (*Running*) or (*Stopped*).

KNM system service status Shows, if the *Kerio Network Monitor Daemon* is installed as a system service *Installed (SVC)* — in Windows NT/2000/XP, as background appli-

5.3 Initial Configuration

cation (*Installed (APP)* — in Windows 9x/Me) or is not installed as service (*Not installed (SVC)*).

Start Runs the service (if stopped).

Reinitialize the service Reinitialization of the service (de facto stopping and rerunning) — only when the service is already running.

Stop Stops the service (if running).

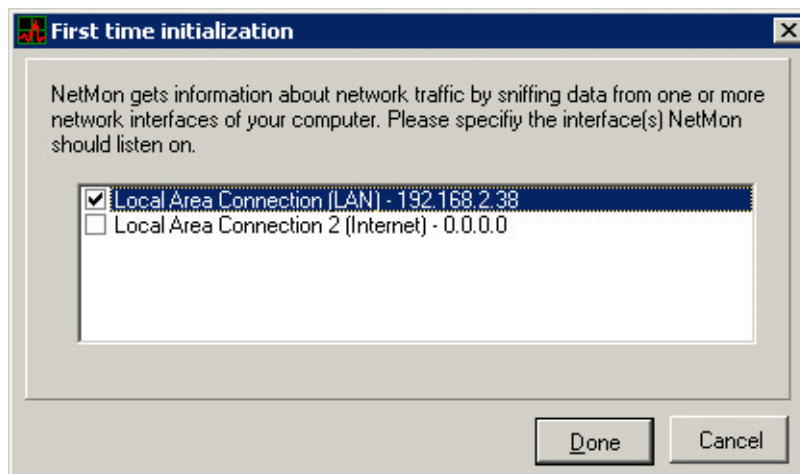
Install as system service Creates the *Kerio Network Monitor* service, if it already does not exist (in Windows NT/2000/XP as system service, in Windows 9x/Me as background application).

Remove the KNM service Removes the *Kerio Network Monitor* system service. The service can be removed only when the service exists in the system and is stopped.

Warning: If the *Kerio Network Monitor Daemon* is installed as the service in the operating system Windows NT/2000/XP, it is possible to start, stop and restart the service also using the system Control Panel *Services*.

5.3 Initial Configuration

If you login to the viewer for the first time (after installation of *Kerio Network Monitor*), a special dialog for selection of the adapters, on which the packets will be monitored, is displayed..



Check the checkbox in front of all of the adapters you want to monitor. Usually it should include all the adapters connected to the local network. There is usually no use of monitoring the packets on the adapter connected to the Internet

Chapter 5 Program Control

if the network address translation is used (NAT), we can see only the address of the computer, which *Kerio Network Monitor* is running on.

By pressing the *Done* button, the settings will be stored and the viewer itself will start. This dialog will not be displayed on any other login. The settings can be, of course, modified in the program.

Chapter 6

Configuration

All settings of *Kerio Network Monitor* are done in the *Configuration* window, which can be accessed by choosing *Settings / Configuration* in the main menu or by pressing the *Ctrl+S* shortcut.

Note: All settings in the *Configuration* dialog have immediate effect (after pressing the *OK* button). In any case there is no need to restart the *Kerio Network Monitor Daemon* service.

6.1 IP Addresses Ranges

The *IP Addresses* tab allows the user to choose network interface, which will be the packet captured on. It also allows definition of IP addresses range, which they will be logged within.

Capture packets from interfaces Usually, it should include all the adapters connected to the local network. There is usually no use of monitoring the packets on the adapter connected to the Internet — if the network address translation is used (NAT), we can see only the address of the computer, which the *Kerio Network Monitor* is running on.

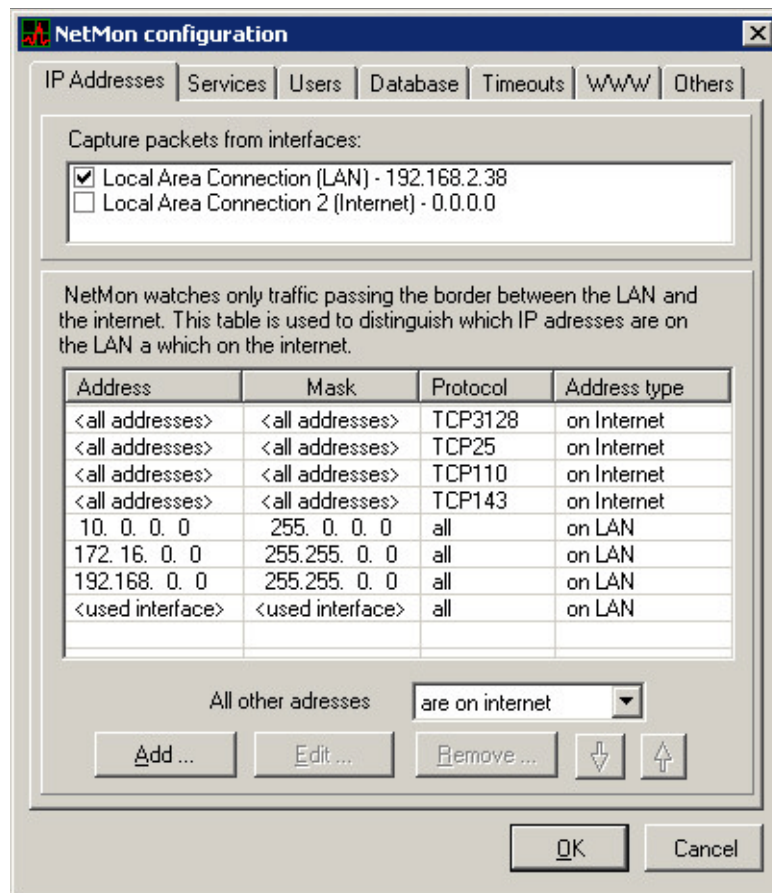
List of IP addresses groups List of individual groups of IP addresses with the group type (*on LAN*, *on Internet* or *discard packet*). Detailed description is later in this document.

All other addresses This option specifies a group, which includes all IP addresses, which do not comply with any of the introduced specifications.

Typical usage example: we specify addresses belonging to the local network and using this option we set that “all other addresses belong to the Internet ” (*are on Internet*).

Add, Edit, Remove These buttons are used for adding new group of addresses, respectively for modification or deleting of the selected group.

Arrow buttons (up / down) The list of IP addresses definitions is always traversed from up to bottom. Therefore the definitions must be ordered from the most specific



to the most general. The arrow buttons are used for moving the selected definition up or down in the list.

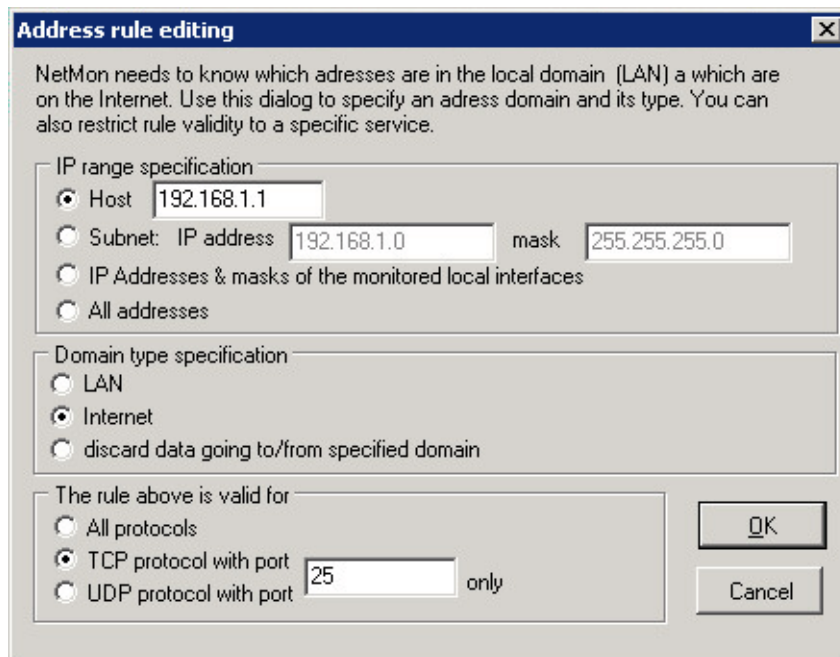
Definition of IP Addresses Group

After pressing the *Add* or *Edit* button the dialog for IP addresses group definition will appear.

IP range specification Type of the group. One of the following types can be chosen:

- *Host* — IP address of a particular computer
- *Subnet: IP address / mask* — IP subnet with appropriate mask.
- *IP addresses & masks of the local interfaces* — all IP addresses of the network, which are connected to the adapters selected for packets monitoring, will be added to the group.
- *All addresses* — all IP addresses

6.1 IP Addresses Ranges



Domain type specification Type (domain) of IP addresses group. This option defines, how will the packets, whose source and target address belong to this group, be processed. The group of addresses can be included in one of the following domains:

- *LAN* — local network. The specific property of this group is that all captured addresses from this group are added to the list of computers (see chapter 7.1).
- *Internet* — addresses from this group are measured but no list is created from them.
- *discard data*
if source or target address belongs to this group, the volume of the data in this packet will not be counted.

Note: The volume of the data in the packet will be measured only when one of the addresses (source or target) in the packet header belongs to the group *LAN* and the other to the group *Internet*. Details are to be found in the chapter 3.2.

The rule above is valid for Specification of the protocol and the port, which is this rule valid for. This way it is possible to define e.g. that only data for particular service will be measured.

- *All protocols* — the rule will be valid for all protocols (and therefore also for all services)

Chapter 6 Configuration

- *TCP protocol with port* — the rule will be valid only for the TCP protocol and the given port. The protocol and the port define particular service (e.g. SMTP, WWW, etc.) The port number 0 (zero) means all ports — so all services using the TCP protocol.
- *UDP protocol with port* — the rule will be valid only for the UDP protocol and the given port. The similar considerations are valid as in the case of the TCP protocol.

Note

After installation of *Kerio Network Monitor*, there are some predefined groups of addresses in the *IP Addresses* tab. They are intended to maximally simplify the program configuration — so that it should be usable with the default settings in the highest possible number of standard situations,

- Rules for all addresses (*<all addresses>*) with specified protocols and ports. These rules specify the services, which are running in the local network but should be monitored as the Internet ones (typically the proxy server and the mail server)

If your network is connected to the Internet via proxy server, the rule for the proxy server should be defined (otherwise no data will be measured because the communication between the client and the proxy server takes place only in the local network). The default rule supposes the standard port 3128 (*TCP3128*). If the proxy server in your network is running on another port (e.g. 80 or 8080), correct the port number in this rule.

If the mail server is running on the computer, which is also the Internet gateway, then *Kerio Network Monitor* can not measure the volume of sent and received mail, because it is communication within the local network. For this reason there are predefined rules for the SMTP (*TCP25*), POP3 (*TCP110*) and IMAP (*TCP143*) protocols.

- Rules for private ranges of IP addresses (10.0.0.0, 172.16.0.0 and 192.168.0.0). These addresses are reserved for private network and can not appear anywhere in the Internet, therefore *Kerio Network Monitor* automatically supposes, that it deals with local network.
- Rule for adapters, which are the packets captured on (*<used interfaces>*).

As it was already described earlier (see chapter 5.3), the packets should be monitored on the interfaces connected to the local network (so that *Kerio Network Monitor* could detect IP addresses of individual computers in the network). Therefore it is supposed that the adapters, which were chosen for packets monitoring, are connected to the local network (domain LAN).

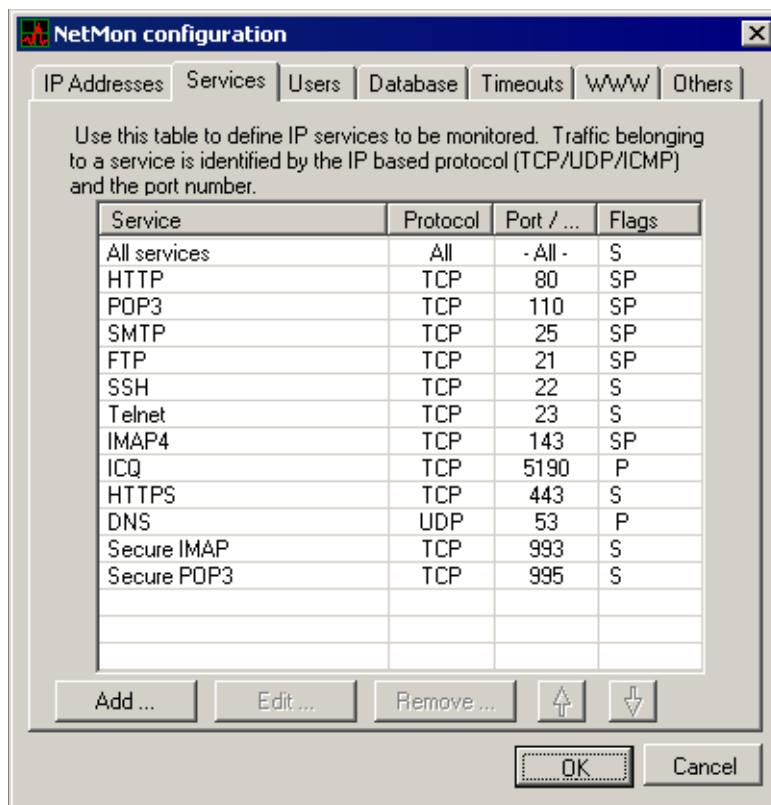
6.2 Monitored Services

If your network is not created from cascading segments (e.g. more subnets interconnected by routers), you have not to define any other rule for IP addresses.

All the predefined rules can be modified or deleted if they do not meet the particular configuration. Usually it is not necessary — if there are e.g. in the local network used only the IP addresses from the range 192.168.0.0, the rules for other private ranges (10.0.0.0 and 172.16.0.0) are not efficient, because those addresses *Kerio Network Monitor* never captures. Similar consideration is valid also for the mail and the proxy server.

6.2 Monitored Services

Kerio Network Monitor allows to define network services, which will be monitored in detail. For this purpose serves the *Services* tab in the configuration dialog.



Chapter 6 Configuration

List of services The window shows the list of the defined services (in the default settings, there is already predefined the majority of the standard services). The columns of the list have the following meaning:

- *Service* — name of the service (given by its definition)
- *Protocol* — protocol, which the service uses (TCP, UDP, ICMP, PPTP or any— *All*)
- *Port / Subprotocol* — port, which is used by the service (only for the TCP and UDP protocols)
- *Flags (flags)* — indication of other parameters, which were set for the service. Details see later.

The buttons under the list of the services allow definition of new service (*Add*), modification of the service settings (*Edit*) or deleting of the service (*Remove*).

The arrow buttons (up / down) serve for ordering the services in the list. This order is important only for better orientation; it has no influence to the function of the program.

Note: With some of the predefined services (*HTTP*, *SMTP*, *POP3*, *IMAP4*, *FTP* and *DNS*) are connected some other functions of *Kerio Network Monitor*, and therefore they can not be removed.

Service Definition

After pressing the *Add* or *Edit* button, the dialog for service definition will be shown:

The dialog box titled "Enter the service parameters" contains the following fields and options:

- Protocol specification:**
 - All traffic of protocol type
 - with port / subprotocol number (0 = All)
 - should be monitored as service
- Protocol options:**
 - Allow protocol statistics
 - Do the detailed protocol analysis
 - Enable protocol debugger for the tech. support
 - Do not delete the debug info

Buttons:

All traffic of ... protocol type Protocol, which is used by the given service. The possibilities are: *TCP*, *UDP*, *ICMP* (Internet Control Messages Protocol), *PPTP* (Point to Point Tunneling Protocol) and *All* (any protocol — i.e. whole IP communication).

with port / subprotocol number Port number, which is used by the service (e.g. 25 = SMTP, 80 = WWW etc.). The value 0 (zero) means all ports (i.e. all communication with the selected port).

Allow protocol statistics Separate logging of the data for this service. In the graph or in the report, it will be possible to separately display the volume of the data transferred only by this service (for details see the chapters 7.2, 7.6).

If this option is on, attribute *S* appears in the column *Flags*.

Do the detailed protocol analysis Performs the detailed analysis of this service. This option is available only for the standard services, where *Kerio Network Monitor* can perform the analysis (*HTTP*, *SMTP*, *POP3*, *IMAP4*, *FTP* and *DNS*). The analysis results (i.e. e.g. captured WWW pages, E-mail messages, transferred files, etc.) are displayed to the *Scanned data* window, or possibly also to the appropriate log (*HTTP Log*, *Mail Log*, *ICQ Log*). Details are to be found in the chapters 7.4 and 7.7.

If this option is on, attribute *P* appears in the column *Flags*.

Note: To define other parameters for protocol analysis use the *Others* option. To see their detailed description refer to chapter 6.7.

Enable protocol debugger Detailed log of data for this service for purposes of technical support. This option can be used if you suspect that *Kerio Network Monitor* does not log the data of appropriate service correctly. Obtained data can be handed to technical support of the *Kerio Technologies* for further analysis.

If this option is on, attribute *D* appears in the column *Flags*.

Do not delete the debug information The detailed data of the service, stored for debugging purposes (see the previous option), are rather large and could very quickly fill in considerable amount of disk space. Therefore they are under normal conditions deleted on each close of the monitored connection. By setting this option on, the data will not be deleted automatically and will remain stored until manually deleted.

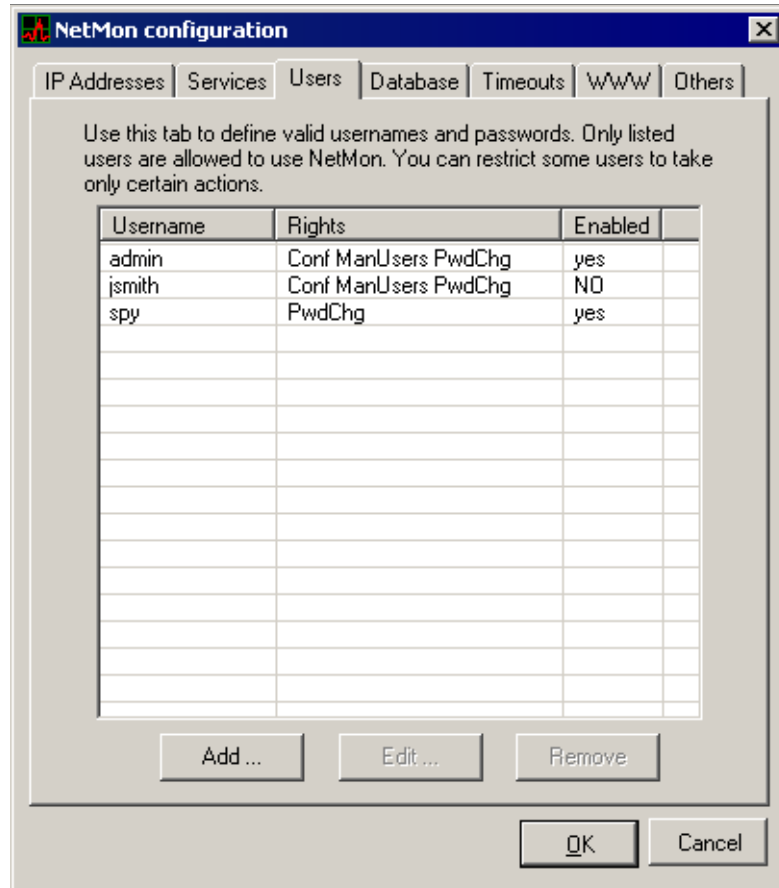
6.3 User Accounts

When the viewer is connecting to the *Kerio Network Monitor Daemon* service, the user name and the password are required. It ensures that only the authorized users have

Chapter 6 Configuration

access to the data and the program configuration and no data breach or its intentional falsification by changing the configuration, should appear.

Any number of user accounts with different levels of access rights can be defined in *Kerio Network Monitor*. There is a tab *Users* for this purpose in the configuration dialog (this tab can be also opened using the *Settings / Users*) menu.



The list of users in this tab includes the following information:

Username User name (which the user logs in with)

Rights Access rights of the user (for details see below)

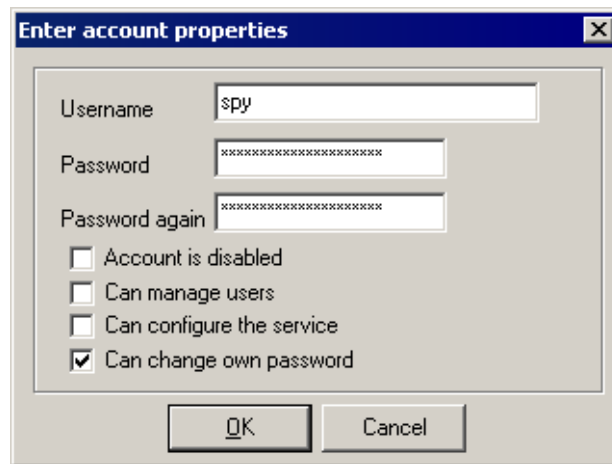
Enabled Account state: enabled (*yes*) or blocked (*no*)

The buttons under the list of the accounts allow definition of new user (*Add*), modification of settings for the selected account (*Edit*) or deleting the account (*Remove*).

Note: The predefined user account Admin can not be removed, assigned access rights or disabled.

User Definition

The dialog for definition of the user account will be shown after pressing the *Add* or *Edit* buttons .



Username Name of the user. It should not contain blanks and punctuation marks. Small and capital letters are not distinguished.

Password The user password. Can contain any printable characters (including spaces); distinguishes capital and small letters.

Password again Verification of the password (to check that no mistakes occurred when entering the password)

Warning: For security purposes, it is recommended not to leave the password empty! Also the password of the predefined user *Admin* should be changed after the first logon.

Account is disabled It is possible to temporarily deactivate (“turn off”) the user account by setting this option on.

If this option is on value *NO* appears in the column *Enabled* in the list of the users , in the other case the value is *yes*.

Can manage users The user is allowed to create, modify and delete the user accounts.

This option also activates the option *Can configure the service* and in the column *Rights* in the list of the users is displayed as *ManUsers* (resp. *Conf ManUsers*).

Can configure the service The user can perform the configuration of the *Kerio Network Monitor Daemonservice*(i.e. all settings in the dialog *Configuration* with exception of the *Users* tab).

Chapter 6 Configuration

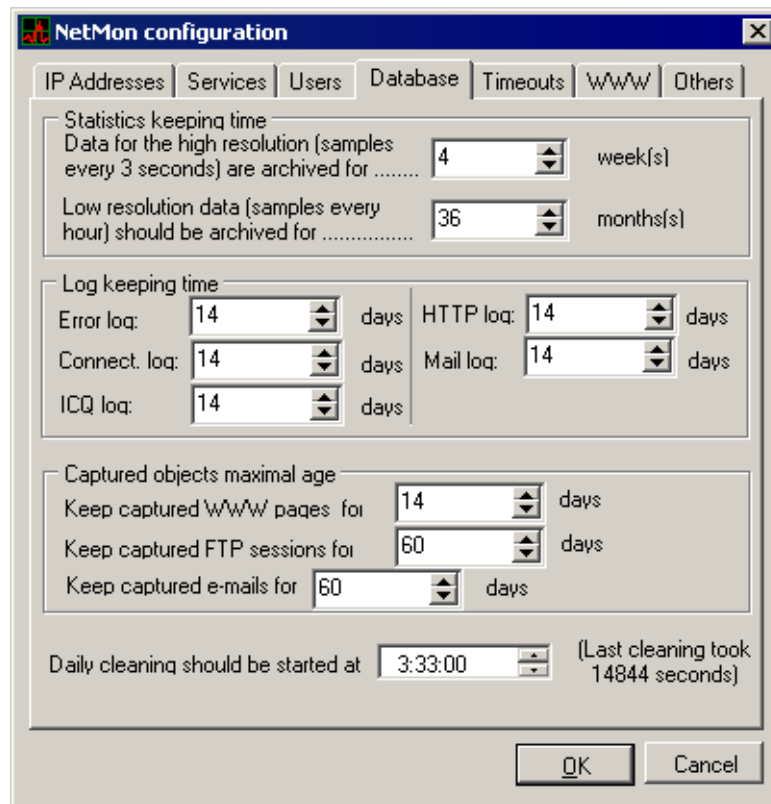
This right is in the column *Rights* in the list of the users shown as *Conf*.

Change own password The user has the right to modify his own password (in the menu *Action / Change password*). If the option *Can manage users* is on, turning the option on or off has no effect.

This right is not shown in the column *Rights* in the list of the users.

6.4 Log Settings

The *Database* tab is intended for setting the parameters for storing the acquired data.



Statistics keeping time The maximum time which will be the statistics — the volume of transferred data in total and for particular defined services — kept for. The optimal setting depends both on the requirement how long should be the measured data stored, as well as on the size of available disk space and on the intensity of the network traffic (during the time of no communication, nothing is stored).

The time for keeping of the data is determined by the two following parameters:

- *Data for the high resolution* — data with the high resolution (3 seconds sampling rate). The time for keeping is given in *weeks*. This data represents the majority of the stored data.
- *Low resolution data* — data with low resolution (1 hour sampling rate). This data occupies much less space than the data with high resolution but its accuracy is sufficient for observing longer time period (e.g. 1 week and more).

Thanks to their small size, the data with small resolution can be kept for longer time — time is given in *months*.

Log keeping time Time of storing (respectively maximum age) of the log files *Error Log*, *Connection Log*, *HTTP Log*, *Mail Log* and *ICQ Log*. Given in *days*.

Captured objects maximal age Time for storing of the captures objects (i.e. information, which is displayed in the window *Scanned data* — see chapter 7.4). Given in *days*.

- *Keep captured WWW pages* — time for storing the captured WWW pages. WWW pages can contain big amount of graphics and other objects, therefore it deals with high volume data.
- *Keep captured FTP sessions* — time for storing the information about connections to the FTP servers. Only information about the relations is stored (server, user, downloaded or uploaded files), not the transferred files. The volume of the data is therefore small.
- *Keep captured e-mails* — time for storing the captured E-mail messages. The messages are stored also with the attachment and can therefore represent high amount of data.

Daily cleaning should be started at Startup time for automatic database maintenance (performed once a day). The main goal of this action is to remove the data, which is older than the set values (see the options described above).

This maintenance can take a long time (in the worst case even several tens of minutes — depends on the size of the stored data and speed of the used computer). During the maintenance time it is not possible to view the currently processed log (in the appropriate window a message saying the maintenance is running, will appear). For this reason, the maintenance should be scheduled to the time, when there is low or even no traffic in the network (e.g. during the night).

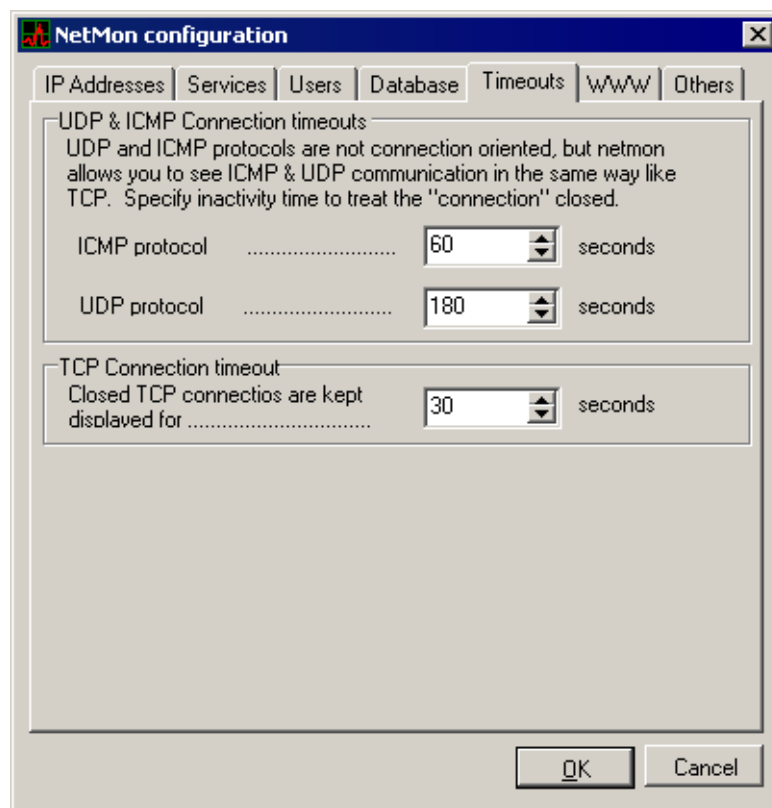
Chapter 6 Configuration

Note: If the computer with *Kerio Network Monitor* is turned off in the given time, maintenance will be performed on the next start of the *Kerio Network Monitor Daemon* service.

(Last cleaning took ... seconds) The time which took the last database maintenance (in seconds).

6.5 Protocol Monitoring Parameters

The *Timeouts* tab serves for setting the time parameters of the individual protocols:



UDP & ICMP connection timeouts The UDP and ICMP protocols are datagram oriented — communication is based on the exchange of individual messages (so called datagrams) among that exists (at the level of the network communication) no connection. The typical communication consists of one or several sequences request — response. Therefore we can suppose there is regular exchange of datagrams in small intervals, in fact it makes one relation (so called pseudorelation). If the interval is noticeably higher, we suppose new relation was started. This principle can be used for showing the UDP and the ICMP pseudorelations in the *Current connections* window (see chapter 7.3).

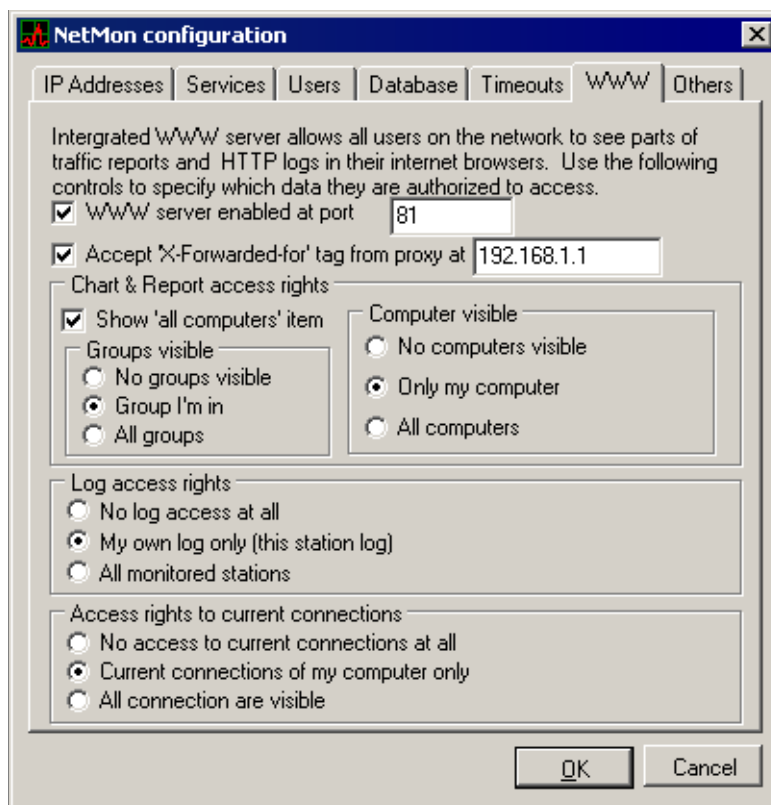
6.6 WWW Interface Parameters

The *ICMP protocol* and *UDP protocol* options are used for setting the above described intervals .

TCP connection timeout The TCP protocol is relation based (first the relation, which the data is transferred in, is created). In this case we know exactly the time of creating and dropping the connection. If a small amount of data is transferred using a fast line the connection can last only a small time (often less than 1 second). In order to enable the user to watch the connection in the window *Current connections* (see chapter 7.3), it is left displayed for some time after the end of the connection. This time is set by the *Closed TCP connections are kept displayed for* option.

6.6 WWW Interface Parameters

The *WWW* tab serves for setting the parameters of *Kerio Network Monitor* WWW interface.



WWW server enabled at port This option enables/disables the embedded WWW server. If set off, WWW interface is not available.

Here is also specified the port, which is the WWW server running on (default 81). If there is no other WWW server running on the computer where *Kerio Network Monitor*

Chapter 6 Configuration

Daemon is installed, it is possible to use the standard port 80 — then it will be no longer necessary to specify the port in the browser, when connecting to the WWW interface of *Kerio NetworkMonitor*.

Accept 'X-Forwarded-for' tag... This option enables the *Kerio Network Monitor* to get the IP addresses of the client computers from the X-Forwarded-for tag in the HTTP request, which was accepted by the embedded WWW server from the proxy server.

Set this option in case that local computers use a proxy server for the Internet access. In this configuration *Kerio Network Monitor* “sees” only the requests from the proxy server. In the X-Forwarded-for tag (which is added by the proxy server), it is possible to find the IP address of the client — the real originator of the HTTP request.

Enter the IP address of the proxy server, which should *Kerio Network Monitor* accept the X-Forwarded-for tag from (it can not be accepted from any proxy server, because this feature could be misused by the clients easily) to the appropriate field. If the proxy server is running on the same computer as the *Kerio Network Monitor Daemon*, use the loopback address 127.0.0.1.

The above described problem can be solved by setting the WWW browser so that it does not use the proxy server for local address (but this option can usually be changed by the users).

The following options define the behavior of the WWW interface if it is opened by the anonymous user (i.e. is not logged in with the user name and the password — see chapter 8.1).

The default setting supposes that each user can view only information about his own computer (that, which is he connected to the WWW interface from). If the user has appropriate access rights to *Kerio Network Monitor* (i.e. has created the user account — see chapter 6.3), he can log in and see all the information, which *Kerio Network Monitor* offers.

Show 'All computers' item The option *All computers* will be shown in the list of the computers (i.e. show the statistics for all of the computers, logged by *Kerio Network Monitor*).

Groups visible Option determining, which groups can be seen by anonymous users (*No groups visible* — no groups, *Groups I'm in* — only the group, which the computer, that is connected to the interface, belongs to or *All groups* — all groups).

Computers visible This option determines, which computers can be seen (*No computers* — no computers, *Only my computer* — only the computer, which he is connected from or *All computers*—all computers).

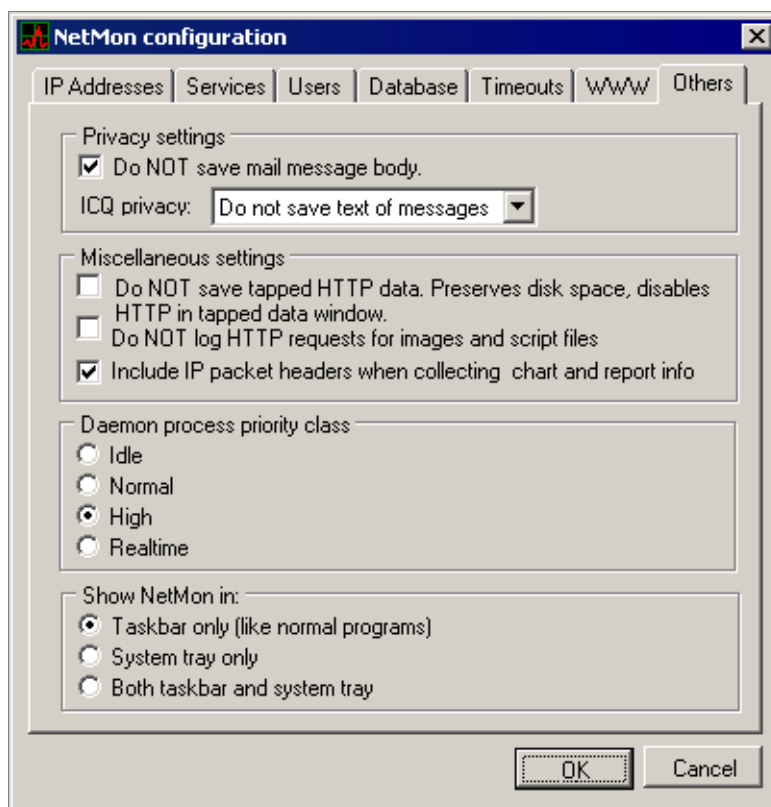
6.7 Additional Settings

Log access rights Access rights to the logs (*No logs access at all* — no logs, *My own logs only* — only logs for the computer which he is connected from or *All monitored stations* — logs for all registered computers).

Access rights to current connections Access rights for monitoring the current connections (*No access to current connections at all* — no connections, *Current connections of my computer only* — only the connections for the computer, which is he connected from or *All connections are visible* — connections for all registered computers).

6.7 Additional Settings

Setting the additional options for appearance and behavior of *Kerio Network Monitor* can be done on the *Others* tab.



Do NOT save mail message body *Kerio Network Monitor* will not store the contents of captured E-mail messages (only the sender and the recipient address are stored).

Note: Monitored and stored can be only messages, which are not transferred using encrypted protocols (in the other case only amount of transferred data can be measured).

Chapter 6 Configuration

Warning: Keep in mind that monitoring the contents of E-mail violates user privacy! If this option is not enabled, all the users should be informed that their mail is monitored!

ICQ privacy Use this option to define how communication through *ICQ* and *ICQ2Go* protocols will be monitored:

- *No privacy* — all transferred data will be monitored (ICQ numbers, nicknames, message bodies)
- *Do not save text of messages* — *Kerio Network Monitor* will not store content of individual messages (only ICQ numbers and nicknames will be monitored)
- *Disable ICQ analyser* — data transferred through *ICQ* and *ICQ2Go* will not be analysed.

Note: This can be also done by disabling detailed protocol analysis in *ICQ* definition (see chapter 6.2). This implies that monitoring is enabled only if either the *No privacy* or the *Do not save text of messages* is used and if detailed protocol analysis is not enabled in *ICQ* configuration.

Do NOT save tapped HTTP data *Kerio Network Monitor* will not store the content of the captured WWW pages. Enabling this option can radically save disk space of the computer. The option HTTP will not be available in the *Tapped data* window(it will not be possible to view pages visited by individual users).

Note: Monitored and stored can be only pages, which are not transferred using encrypted protocol HTTPS (in the other case it is possible only to measure the volume of the transferred data).

Do NOT log HTTP requests for images... When opening the WWW pages in the browser, an HTTP request must be sent for each object contained in the page (picture, script, etc.). In the *HTTP Log* are by default logged all the HTTP requests. Enabling this option makes only the pages themselves to be logged — *HTTP Log* will be much shorter and easier to read. Such HTTP log is sufficient enough in the majority of cases.

Note: The log of requests to window / file *HTTP Log* can be done only if the communication is via the HTTP protocol. In case of the encrypted HTTPS protocol only the volume of transferred data is logged.

Include IP packet headers... Enabling this option causes the total size of transferred data to be counted from whole IP packets including the headers. Its use depends on the data you want to get.

6.7 Additional Settings

Note: If you want to compare data acquired by *Kerio Network Monitor* with data from other programs or with the data from the Internet provider, it is necessary to find out, which methods are used for getting them and set the option *Include IP packet headers* of *Kerio Network Monitor* in accordance.

Daemon process priority class *Kerio Network Monitor* priority definition. The *high* priority is set by the default. We recommend you to change this status under the following conditions only:

- the service overloads the system — set lower process priority
Note: This solution is temporary only — we recommend you to use more powerful hardware.
- packet loss is often reported in the *Error Log* for lack of system capacity (refer to chapter 7.7) — set higher process priority

Show NetMon in This option defines how should the *Kerio Network Monitor* be represented: *Taskbar only* , *System tray only* or *Both taskbar and system tray* (both places).

Chapter 7

Viewing and Analysis of Captured Data

Kerio Network Monitor offers several tools for the presentation and analysis of the captured data. These functions can be chosen from the *View* menu or directly from a toolbar icon (the order of the functions is the same):



Traffic chart Chart of the transferred data volume. You can display a transferred data for the chosen time interval in several graphical representations. The incoming and outgoing data, the particular computers, groups etc. can be watched separately.

Current connections Displays current connections from particular computers. The window content is periodically refreshed.

Scanned data Displays the logged data from specific protocols (WWW pages, e-mail messages, FTP sessions etc.)

Status window Status of the *Kerio Network Monitor Daemon* service (logged user, statistics of captured packets, disk volume occupied by the stored data...)

Report Creates a well-structured table from the transferred volume of data according to the specified parameters (time period, type of operation, level of details...)

Connection log Displays the log of connections from particular computers (history of the *Current connections* window)

HTTP log Log of requests from particular computers to WWW pages, or to all HTTP objects, respectively. (see chapter 6.7)

Mail log Log of the captured e-mail messages (e-mail address of a sender and recipient, subject, and message size)

ICQ log Log of ICQ messages (ICQ numbers, user nicknames and message contents)

Error log Log of errors and warnings. The *Kerio Network Monitor* administrator should study this log regularly and try to eliminate detected errors and problems.

Chapter 7 Viewing and Analysis of Captured Data

KNM access log Log of information on users connecting into the application and on access to the Web interface. Each row includes a corresponding date, time and information on the following issues:

- user's login (username and DNS name or IP address of the host from which he/she connects)

Note: Failed login attempts are also logged — for example, you may find a log informing that an unauthorized person tried to connect.

- demand on the Web interface page (DNS name or IP address of the client, username, HTTP method and URL of demanded Web page)

All the functions described above behave in the following manner:

- If the relevant window is not open, then the window is displayed after the icon is clicked (or after the menu item is selected).
- If the relevant window is already open, then it is activated and moved to the front.
- If you select the function while you simultaneously press the *Shift* key, the new window for this function is displayed.

Hint: The third described way can be used to open vertically or horizontally arranged charts for the incoming and outgoing traffic.

7.1 List of Computers

Left column of the main *Kerio Network Monitor* window shows the list of particular computers in a local network. The list is created automatically from the data of the captured packets. The computer is included in this list if the following conditions are met:

- IP address of the computer belongs to the group *LAN* (see chapter 6.1)
- *Kerio Network Monitor* has already logged at least one packet with the header containing this IP address (as a source or target address) — in this way, it learns that a computer with this IP address exists.

If possible, the detected IP address is translated to a computer name (using reverse DNS query) and the name is displayed. In the other case, the directly detected IP address will be shown in the list of computers.

7.1 List of Computers

Use of List of Computers

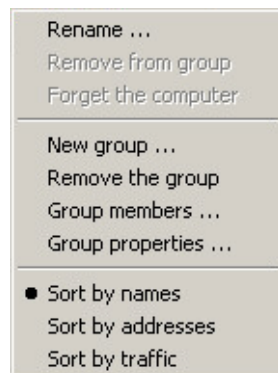
The list of computers is important for presentation of chart (see chapter 7.2) and table of transferred data volume (see chapter 7.6) presentation. These functions can display data either for all computers in a local network (*All computers*) or for only the selected computer (computers, respectively). Computers in the list can be arranged to groups (see later). One computer can act as a member of more groups.

A computer/computers can be selected by mouse click. Several computers (and/or groups) can be selected with the *Shift* key pressed simultaneously. A circular field beside a computer name (or a group) shows, whether it was selected or not.

A sufficiently contrast color (as compared to the chart background or to the other, already applied colors) will be assigned to the selected computers. This color will be used to separately show values for the selected group of computers in the chart.

Management of List of Computers

The user can right-click to the list of computers, or directly to the selected computer or group, respectively. The menu with functions for the list of computers will be displayed.



Rename Renames the selected groups or computers. This function is reasonably especially for computers — the automatically detected name does not have to be descriptive enough or known at all (there is an IP address displayed in the list).

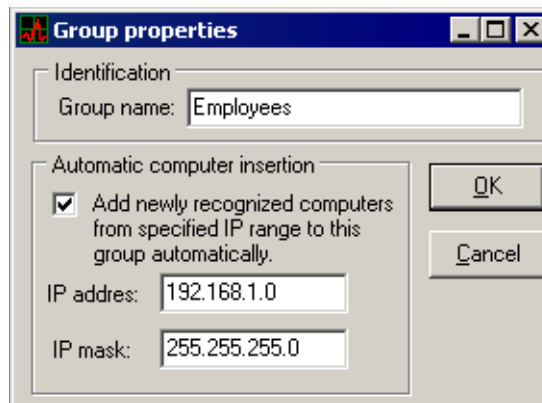
Remove from group Removes the selected computer from the group, which it belongs to.

Forget the computer Deletes the selected computer from the list. This function can be helpful, e.g., when the computer is permanently disconnected from a network, or the IP address was changed.

Chapter 7 Viewing and Analysis of Captured Data

Note: If the packet with the same IP address is detected anytime afterwards, the computer will be automatically included again.

New group Creates a new group. The dialog for a creation or a change of a group contains the following parameters:



- *Group name* — name of the group. It should be sufficiently descriptive (i.e. it should reflect, in general, the type of computers that will be included in this group).
- *Add newly recognized computers* — when this option is checked, all new detected computers (IP addresses) from a specified subnet will be automatically added to this group. Enter the requested subnet with the appropriate mask.

Note: This option can be checked for several groups simultaneously, even for the same subnet.

Remove the group Remove the selected groups from the list. This option does not delete the computers which belong to the group, it only cancels their membership in this group.

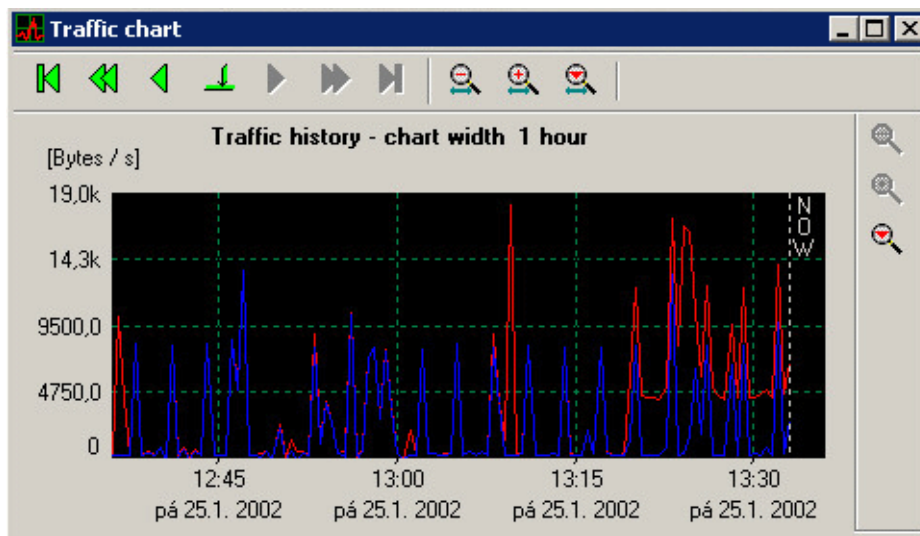
Group members A simple dialog that can be used to add or remove computers from/to the selected group.

Group properties A dialog for a change of parameters of the selected group (identical to the dialog for creation of a new group — see above).

Sorting of list of computers The last three options in the menu determine sorting of the list of computers: by names (*Sort by names*), by IP addresses (*Sort by addresses*) or by a transferred data volume in a descending order (*Sort by traffic*).

7.2 Traffic chart

Shows the chart of transferred data. The horizontal axis shows time, the vertical axis the connection load (in bytes per second).



Buttons with arrows above the chart moves the vertical axis (from left to right):

- Jump to the beginning of the chart (i.e. the whole time interval, when the data was captured)
- Long jump backwards
- Short jump backwards
- Jump to the specified position (date and time)
- Short jump forwards
- Long jump forwards
- Jump to the end of a chart (i.e. the current time)

Note: The length of a short and long jump depends on a scale of the chart.

Buttons with a magnifying glass above the chart set the scale of the x-axis — i.e. the time interval that will be presented in the chart. The displayed interval can be between 1 minute and 1 year.

Buttons with a magnifying glass right to the chart set the scale of the vertical axis. Moreover, there exists an option *Auto*, which automatically adjusts the scale of this

Chapter 7 Viewing and Analysis of Captured Data

axis to the maximum captured value in the given representation (the option is implicitly turned on). This guarantees good readability of the chart.

Right mouse click in the chart area shows a menu with the following items:

Save chart as picture Saves the chart as a picture in JPEG or BMP format.

Zoom in, Zoom out Zooms in/zooms out the scale of the horizontal axis (time interval). The functionality of these options is the same as the functionality of the buttons “magnifying glass +” and “magnifying glass -” above the chart.

View mode The user can switch between the following view modes:

- *Sum of incoming and outgoing traffic* — One line representing the sum of the incoming and outgoing data volume will be displayed in the chart (default setting)
- *Incoming traffic* — only the volume of the incoming (downloaded) data will be displayed in the chart
- *Outgoing traffic* — only the volume of the outgoing (sent) data will be displayed in the chart
- *Both directions at once* — two lines will be displayed in the chart — one for the incoming and the second for the outgoing traffic

Type of chart The chart can be displayed in one of the following forms:

- *Draw lines* (default setting)
- *Draw bars*
- *Draw polygons* — stacked area (area under the line)

7.3 Current Connections

The *Current connections* item shows the window with current connections. This window contains information about the current TCP connections, or UDP and ICMP pseudoconnections, respectively, from particular stations in a local network.

The *Current connections* window contains a tree with two top-level items:

- *All computers* — this option shows all computers which are in the *Kerio Network Monitor* database (see chapter 7.1).
- *Groups* — particular groups (defined in the list of computers) are presented here.

7.3 Current Connections

The screenshot shows a window titled 'Current Connections' with a 'Refresh periodically' checkbox checked. The main area displays a tree view of computers and their connections. The 'All computers' group is expanded, showing four computers: benny, medi, richard, and zdenci. The 'zdenci' computer is selected, and its connections are listed below it. Each connection is represented by a green double-headed arrow icon and a text line showing the protocol, local address, remote address, and data transfer statistics.

Computer	IP Address	TCP	UDP	Connections	Data Transfer
All computers		19x	0x	35 +	16B/s
benny	(192.168.2.192)	8x	0x	12 +	5B/s
medi	(192.168.2.45)	4x	0x	2 +	2B/s
richard	(192.168.2.38)	1x	0x	13 +	6B/s
zdenci	(192.168.2.204)	6x	0x	8 +	3B/s

Protocol	Local Address	Remote Address	Data Transfer
TCP	zdenci:3568	12.249.134.106:1214	290 + 183B
TCP	zdenci:3217	205.188.8.197:5190	4231 + 37391B
TCP	zdenci:3555	217.80.243.73:1214	0 + 0B
TCP	zdenci:3566	217.80.243.73:1214	0 + 0B
TCP	zdenci:3569	217.85.175.136:1214	0 + 0B
TCP	zdenci:3556	24.9.26.50:1214	0 + 0B

The *Current connections* window shows only the computers (or groups, respectively) that have at least one connection open (the inactive computers are not displayed).

Computers included in a group are displayed under the group. Particular connections of a computer are displayed under each computer. The log for the concrete connection has the following structure:

```
TCP: zdenci:3568 -> 12.249.134.106:1214 290 + 183B 13 + 23B/s 3 /  
2s Active *unknown*
```

- TCP: — communication protocol (TCP, UDP or ICMP)
- zdenci:3568 — name (or IP address) of a computer in a local network (typically a client) and the port number
- 12.249.134.106:1214 — name or IP address of a computer in the Internet (typically a server) and the destination port
- 290 + 183B — volume of the sent and received data (in bytes)
- 13 + 23B/s — speed of the transfer of the outgoing (sent) and incoming (received) data (in bytes per second)
- 2 + 3s — time of the last data transfer and total time the connection was open (in seconds)
- Active — connection state (Syncing — connecting, Active — active / open, Closing by initiator — terminating by client, Closing by responder — terminating by server, Closed — terminated, !!! ERROR !!! — terminated because of an error).

Chapter 7 Viewing and Analysis of Captured Data

Closed connections remain displayed in the *Current connections* window for time specified in the program configuration (see chapter 6.5).

An error occurs when a packet from a connection is lost and the connection lost synchronization (consecutively, the connection is terminated and the new one is established, if needed).

- *unknown* — name of service (if it is defined in *Kerio Network Monitor* — e.g. SMTP, HTTP, FTP etc.) or *unknown* (unknown service)

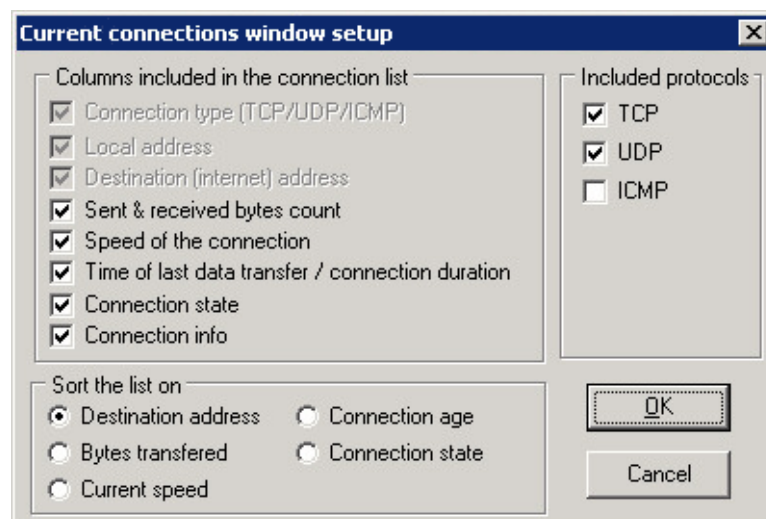
Note: *Kerio Network Monitor* resolves names of computers using an analysis of the DNS protocol. This can be done only if the DNS query was sent before the connection was initiated. If the client has this information in its local DNS cache, the DNS query is not sent and *Kerio Network Monitor* “sees” only the IP address of a destination server.

Current Connections Window

The *Current connections* toolbar contains the following functions and options (from left to right):



Select columns & setup sorting This button opens the dialog window for the *Current connections* window parameters settings.



Columns included in the connection list The user can select which columns (information) will be displayed in the *Current connections* window.

- *Connection type* — type of connection (TCP connection, UDP or ICMP pseudoconnection)
- *Local address* — name or IP address of a local (source) computer and a source port
- *Destination* — name or IP address of a remote (target) computer and a target port

Three functions mentioned above show basic information about the connection and that's why it is not possible to turn them off (hide them).

- *Sent & received bytes count* — number of sent and received bytes
- *Speed of the connection* — speed of data transfer (incoming and outgoing direction)
- *Time of last data transfer / connection duration* — time of the last data transfer and the total time of connection
- *Connection state* — active, closed etc.
- *Connection info* — information about the service (if it is defined in the program)

Included protocols Which protocols shall be monitored in the current connections window. Default settings include the TCP and UDP protocols.

Sort the list on Choice of an item that will be used for sorting of the output in the window (*Destination address* — destination IP address, *Bytes transferred* — volume of transferred data, *Current speed* — speed of the connection, *Connection age* — connection duration, *Connection state* — state of the connection).

Refresh now Updates information in the *Current connections* window.

Refresh periodically When this option is turned on, the information in the *Current connections* window will be refreshed automatically in the periodic time intervals (every 1 second).

7.4 Tree of Scanned Data

Scanned data item opens the window where the captured data of particular services (WWW pages, e-mail messages, FTP relations etc.) can be viewed.

Chapter 7 Viewing and Analysis of Captured Data



Tree of data (in the left part of the window) contains two base branches:

- *By client* — data sorted according to the IP address of clients (i.e. computers in a local network)
- *By protocol* — data sorted by particular protocols (services)

Both branches contain identical data — they differ only in the type of sorting.

The user can expand the selected branch of the tree and click on a concrete object (e.g. WWW page on a given server). This object will be displayed in the right part of the window.

Note: If it is not forbidden in the program configuration (see chapter 6.7), content of e-mail messages will be displayed.

Note #2: For WWW pages, *Kerio Network Monitor* records a particular URL and a page content (HTML code without pictures, applications etc.) When the page is being displayed, the code is opened and the relevant objects are downloaded directly from a server (i.e. in the same way as a browser).

Scanned Data Window

The toolbar of the *Scanned data* window contains the following functions and options (from left to right):

7.5 Status Information



Stop current transfer Stops the transfer of the opening WWW pages (as in a browser)

Refresh tree Updates information in a tree (new data could be scanned since the *Scanned data* window was opened).

This function can be invoked by *F5* key.

Max age The maximum age of data, which should be presented in the tree (in an interval from 5 minutes to one week, or unlimited age — **unlimited**). The Max age option affects noticeably the size and the readability of a tree.

Show formatted Shows formatted WWW pages or e-mail messages

Show as plain text Shows WWW pages or e-mail messages in a text format (source code)

Open as document Opens pages or messages as a document (in a default WWW browser or an e-mail client)

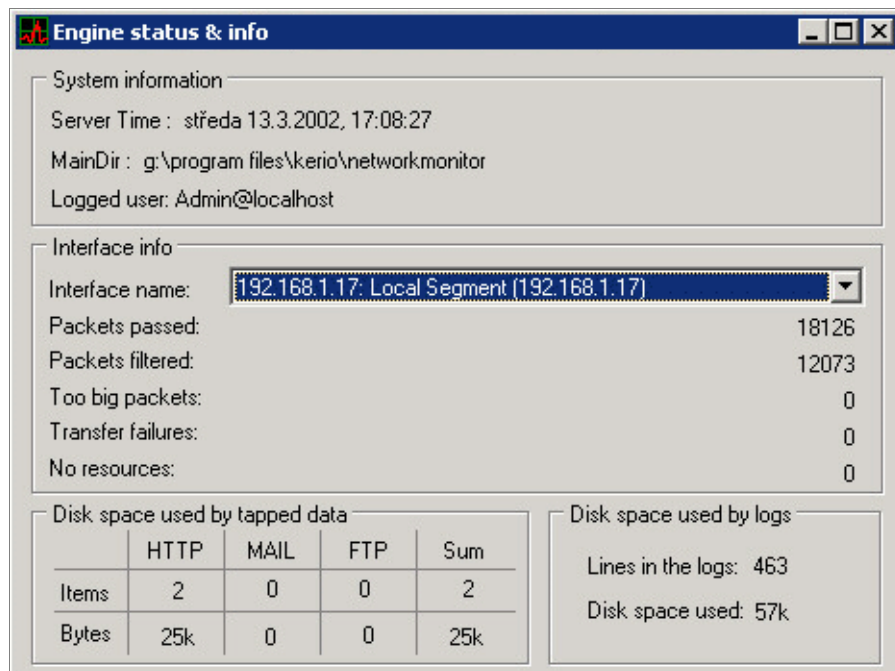
7.5 Status Information

Status window shows information about the system with the *Kerio Network Monitor Daemon* installed, about the network interfaces and the disk space occupied by the database of the scanned data.

System information System information (current time of the server, the installation directory, and the currently logged user). The logged user is displayed in a form `name@server`, where `server` is a DNS name or an IP address of the computer, where the *Kerio Network Monitor Daemon* service runs (to which the user is connected).

Interface info Statistical information about the particular interface where *Kerio Network Monitor* captures packets. All these information are computed from the start of the *Kerio Network Monitor Daemon* service. Statistics are reset after the restart of the server.

- *Interface name* — interface for which the statistics will be displayed. This listbox contains all interfaces selected in the configuration program (see chapter 6.1) for the packet scanning.
- *Packets passed* — total number of packets passed to the *Daemon* for processing (their source and target address belongs to different groups)



- *Packets filtered* — number of filtered (discarded) packets — their source and target address belongs to the same group or some of these addresses belongs to the group *Discard packet* (see chapter 6.1)
- *Too big packets* — number of packets that couldn't be processed because their size exceeded the maximum size of the cache of the low-level driver of *Kerio Network Monitor*. Greater number of these packets can indicate a system error or a possible attack.
- *Transfer failures* — number of packets that were not successfully copied from the internal cache of the network adapter. This error should not occur under normal circumstances (it can indicate a problem with an adapter or its driver).
- *No resources* — number of packets that were not successfully processed due to the lack of system resources.

If this value is in the thousands, *Kerio Network Monitor* should be installed to a more powerful computer or to a dedicated computer where no user works.

Disk space used by scanned data The size of disk volume occupied by captured data from particular services. The number of objects (*Items*) and bytes (*Bytes*) is displayed. The *Sum* column contains the total space occupied (sum of all services).

Note: Presented data doesn't include the space occupied by a database of a volume of transferred data (i.e. subfolders *high* and *low*).

7.6 Transferred Data Volume Table

Disk space used by logs The total disk space occupied by recorded files and the total number of lines in these files.

7.6 Transferred Data Volume Table

The *Report* function shows - according to the specified parameters - a window with the table of transferred data volume. If the window is not open, the dialog for parameters settings is displayed:

The screenshot shows a dialog box titled "Set report options" with the following fields and controls:

- 1. Set column's options**
 - Number of columns in the report: 8
 - One column contains traffic summary for: 1 hour(s)
- 2. Select report's start date**
 - The report starts on: 1. 6 .2002 at 8:00:00
 - Buttons: Suggest start time, When suggesting, include the current interval (checked)
- 3. Select the service**
 - The report includes network traffic for: All services
- 4. Choose the traffic direction**
 - Radio buttons: Incoming only, Outgoing only, Sum of both (selected)
- Bottom controls: Show percentages (unchecked), OK, Cancel

Set column's option Basic parameters specifying table extent:

- *Number of columns* — number of columns in a table
- *One column contains traffic summary* — time interval which shall be covered by one column

Combination of these two parameters determines the total extent of the table.

Example: We want to display a number of transferred data during one week in one-day intervals. We enter value 7 (week has usually 7 days) to the editbox *Number of columns* and *1 day(s)* to the *One column contains traffic summary*.

Select report's start date Select start time and date (from when the data shall be processed). From that date the time period set in the previous section is interpreted. Button *Suggest start date* sets the start time so the chosen time period ends with the current time.

Chapter 7 Viewing and Analysis of Captured Data

Example: If we set the extent of a table according to the previous example, button *Suggest start date* sets the date and time seven days ago (i.e. the final table will display seven days).

Checkbox *When suggesting, include the current interval* governs whether the suggested start time includes the current interval (which is not finished yet).

Example: Today is Saturday 1st June, 2002, 12:00 p.m. We consider the same interval as in the previous example (i.e. the data for one week in one-day intervals). The *Suggest start time* button sets the last Saturday (i.e. 25th May, 2002). The table will then contain the data for time period from Saturday 25th May, 2002 to Friday 31st May, 2002. If we check the option *When suggesting, include the current interval*, the suggested date will be Sunday, 26th May, 2002 and the table will contain data for the period Sunday, 26th May, 2002 — Saturday, 1st June, 2002. The last column in the table will then contain the data for today (i.e. 0:00 a.m. — 12:00 p.m.). If we let the program create the table with the same parameters e.g. at 6:00 p.m., the data in the last column will be different.

Select the service The user can select a service whose data will be displayed in a table. The concrete service (e.g. *HTTP*, *SMTP*, *FTP* etc.) or all services (*All services*) can be selected.

Choose the traffic direction Chooses the direction of the traffic that should be captured: *Incoming only* (only incoming data), *Outgoing only* (only outgoing data) or *Sum of both* (the sum of outgoing and incoming data).

Show percentages Shows percentages instead of the transferred data for particular computers. If this option is checked, only the total volume of the transferred data for the relevant time period (item *All computers*) will be displayed in the table. The relevant volume of the transferred data will be displayed in percentages for each computer.

The *OK* button creates and shows the table according to the specified parameters.

Functions for the Data Volume Table

The *Accounting report* window toolbar offers the following functions (from left to right):



Change report parameters Changes table parameters. This option shows a dialog for the table settings (see above). When the dialog is closed, a new table is displayed.

Print the report Prints the table. This option opens a standard system print dialog where a printer etc. can be selected.

Save the report Saves the table as an HTML page or in a CSV format (Comma Separated Values). The CSV format is relatively common and it can be opened in a lot of programs (e.g. Microsoft Excel).

Sort the table Sorts the table according to the selected column. This option can be used repeatedly — a new table need not to be created.

Transfer the table to MS Excel If *Microsoft Excel* is installed on the host where the browser is running, you can use this button to transfer the table to the application. *Microsoft Excel* offers a variety of other alternatives of how to process obtained data.

7.7 Log Windows

All log windows — (*Connection Log*, *HTTP Log*, *Mail Log* and *Error Log*) have a toolbar with these functions (from left to right):



Copy selection to clipboard Copies the selected text to a clipboard (mouse can be used to select text). This function can be invoked using the standard hot key *Ctrl+C*.

Save log to file Stores log to a text file in a text format (*.txt) or in a LOG format (*.log). This function can be invoked by the hot key *Ctrl+W*.

In general, the LOG format is more suitable for an automatic processing while the text format is more readable for a user. For HTTP log, the LOG format is a standard (unix) log and the text format preserves the form presented on a screen. All other logs in the LOG format show only IP addresses. In the text format, they are substituted by computer names (if they are known).

Show only lines passing the rule Logs filtering. The user can display only the lines containing the specified string. For example, only the part of the log referring to a specific date can be displayed in this way.

Log Reading and Analysis

Each line of a log contains information about one event (e.g. about e-mail message, HTTP request, error message etc.).

Chapter 7 Viewing and Analysis of Captured Data

Log files can be further processed by external analytical tools (e.g. by *Kerio Log Analyzer* application — see www.kerio.com).

Connection Log

```
TCP: richard:1524 -> 205.107.97.6:80 171 + 2927By,  
2s -HTTP:205.107.97.6
```

- Fri 8/Mar/2002 10:18:31 — date and time of a connection creation (formation)
- TCP: — used communication protocol at transport level (*TCP/UDP*)
- richard:1524 — name or IP address of a client (computer that originated the connection) and source port
- 205.107.97.6:80 — name or IP address of a target computer (server) and destination port
- 171 + 2927By — volume of sent (171) and received (2927) data in bytes (By)
- 2s — connection duration (in seconds)
- -HTTP:205.107.97.6 — service description (if it is a service defined in *Kerio Network Monitor*). This record shows “HTTP service on a server with IP address 205.107.97.6”. If *Kerio Network Monitor* doesn’t have such a service, the error message `unknown service` is displayed.

Note: *Kerio Network Monitor* resolves names of computers in the Internet using a DNS protocol analysis. This method can be used only if a DNS query had been sent before the connection was established. If a client contains this information in its local DNS cache, a DNS query is not sent and *Kerio Network Monitor* “sees” only the IP address of a target server.

HTTP Log

```
richard - Fri 8/Mar/2002 11:57:46  
GET http://www.kerio.com/resources/home.gif  
HTTP/1.1 200 1221
```

- richard — name (or IP address) of a client (i.e. the computer that sent the HTTP query)
- Fri 8/Mar/2002 11:57:46 — date and time of a request

- GET — method of HTTP protocol (*GET/POST*)
- <http://www.kerio.com/resources/home.gif> — complete URL of a requested object
- HTTP/1.1 — HTTP protocol version (currently 1.0 or 1.1)
- 200 — HTTP protocol return code (see document *RFC2068* — www.ietf.org/rfc)
- 1221 — size of an object (in bytes)

Mail Log

richard - Fri 8/Mar/2002 14:26:01

SMTP From: "Richard Gabriel" <richard@kerio.com> ,

to: <info@zaluzi.cz> , subj: Order, 43 lines, 1366 bytes

- richard — name (or IP address) of a client (i.e. the computer that initiated the connection to a mail server)
- Fri 8/Mar/2002 14:26:01 — date and time of a message transfer
- SMTP — used mail protocol (*SMTP*, *POP3* or *IMAP*)
- From: ... — e-mail address of a sender (and his name — if it was specified)
- to: ... — e-mail address of a recipient (and his name — if it was specified)
- subj: ... — message subject
- 43 lines — number of lines in a message body
- 1366 bytes — total size of a message (in bytes)

Error Log

Fri 8/Mar/2002 14:59:59 Warn - 192.168.2.38:

5 packets lost - lack of resources (61-56)

Fri 8/Mar/2002 15:02:11 Warn - (192.168.2.40 -> 201.7.55.112)

Connection has died

Fri 8/Mar/2002 15:17:22 Err: 206 - Error creating file

Chapter 7 Viewing and Analysis of Captured Data

'c:\Program Files\Kerio\Network Monitor\logs\mail.idx'

- Fri 8/Mar/2002 14:26:01 — date and time when the error was logged
- Warn — type of a message (Warn — warning or Err: xxx — error including the error number)

Warnings represent minor errors with smaller importance. The *Kerio Network Monitor* administrator should not ignore these warning and he should try to eliminate all errors.

- 192.168.2.38 — IP address of a computer where the error was logged. Addresses of source and target computers of the connection where an error occurred can be presented here too.
- 5 packets lost - lack of resources (61-56) — detailed error description

Note: There is a large number of errors and warnings that can appear in *Error Log*. Their description goes beyond the scope of this guide. If you are not able to cope with an error yourself, you are advised to contact *Kerio Technologies* technical support — see www.kerio.com.

Chapter 8

Web Interface

Kerio Netwok Monitor provides access to captured data using the basic Web interface. This interface can display a chart of connection load, list of current connections, and a transferred data volume table created according to the specified parameters.

WWW interface operates in two modes: with an anonymous or authenticated user.

- The user can examine only data for his own computer (the computer which is used to connect to the interface), or (if it is permitted) the aggregate data for the whole network, respectively. It is assumed that the user connects to the interface from his “own” computer and he will see only the data exactly for this computer.
- The authenticated user can examine all data provided by *Kerio Netwok Monitor* (i.e. data about all computers in a local network).

8.1 Connection to the Web Interface

The user must enter DNS name of a computer that runs *Kerio Netwok Monitor Daemon* (or IP address if it is not registered in DNS, respectively) and specify the port where the Web interface runs (implicitly *81*) E.g. the URL can look like this:

```
http://server.company.com:81
```

or

```
http://192.168.1.1:81
```

If the computer where the *Kerio Netwok Monitor Daemon* is installed doesn't run another WWW server, the WWW interface can be started on the default port *80* (see chapter 6.6) — port does not have to be specified in the URL:

```
http://server.firma.cz
```

or

```
http://192.168.1.1
```

User Login

The user does not have to explicitly login to the WWW interface of *Kerio Netwok Monitor*. Immediately after the start, the interface operates in an anonymous mode (see above).

Chapter 8 Web Interface

If you want to display data about all computers in a local network, log in the *login* section. Information about all computers becomes accessible after the successful login. In the other case, the WWW interface remains in the anonymous mode.

8.2 Page *Main*

This section shows information about the system where the *Kerio Network Monitor Daemon* runs (system time, license information, used disk space...).

Information on this page (with a few exceptions) corresponds to the *Engine status & info* window — see chapter 7.5.

8.3 Page *Chart*

Page *chart* displays a chart of transferred volume data (as *Traffic chart* window — see chapter 7.6).

Options in a left part of the page set chart parameters:

Select red / blue / green sequence Chart on this WWW page can display at most 3 lines (red, green and blue) - a type of displayed information can be set for each line. The choices are:

- *All computers* — total volume of transferred data for all computers
- Name of computer or group — volume of transferred data for the selected computer or group
- *<none>* — line will not be displayed. This option is available only for the second and the third line (i.e. the green and blue line).

Select chart width Time interval that will be displayed in the chart (from 1 minute to 1 year).

Show Shows the chart with the specified parameters.

Row of buttons is displayed above the chart. They move the chart content alongside the horizontal axis. Middle button *Refresh* is used to refresh the chart (the chart on a WWW page is not automatically refreshed because of technical reasons).

8.4 Page *Report*

This page corresponds to the *Accounting report* window. Before the page is opened, the options for table parameters settings are displayed:

Select format Formats of the table (HTML page or file in CSV format)

Specify report parameters Table parameters settings (see chapter 7.6).

Show the report Shows the table of transferred volume data according to the specified parameters.

8.5 Page Connections

This page shows current connections of particular computers — it is an equivalent of the *Current connections* window. Page can not be configured.

Details how to show current connections can be found in chapter 7.3.

8.6 Page Logs

This page shows the selected information from *HTTP Log*, *Mail Log*, and *Connection Log* (*Error Log* can be displayed only in the application).

Select log Selects log (*HTTP Log*, *Mail Log* or *Connection Log*).

Specify log options Specifies parameters for log items that will be displayed:

- *Show last ... days* — show only log items for the last ... days. This option strongly affects the length of the displayed page, therefore we recommend to choose only the time period that is required.
- *at most ... lines* — maximum number of displayed lines
- *Show only lines containing ...* — show only lines containing the specified string (if you want to show all lines, leave the field empty)
- *Resolve IP addresses of local computers* — if this option is checked, the local computers will be displayed as DNS names (if they exist). Otherwise, only IP addresses will be displayed.

Note: Remote computers (i.e. the computers that don't belong to a local network) are always displayed as IP addresses.

Show the log Shows log items according to the specified parameters.

8.7 Integration of the WWW Interface into the Company Website

The WWW interface of *Kerio Network Monitor* enables access to particular pages or their parts using the special URL. Various charts or tables (e.g. chart of connection load, table

Chapter 8 Web Interface

of transferred data volume or view of current connections etc.) can be integrated into your own web site in this way.

General Format of URL

URL of pages from the WWW interface has, in general, this format:

```
http://netmon:81/directory/page  
?parameter1=value&parameter2=value...
```

where:

- `netmon` — DNS name or IP address of the computer, where *Kerio Network Monitor* runs.

Note: Integration into another website must take into consideration if pages will be accessed from an internal network, from the Internet, or from both directions. The best way is to use the name of the server that has the appropriate entries both in the internal and the public DNS.

- `81` — port where the WWW interface of *Kerio Network Monitor* runs (see chapter 6.6)
- `directory` — directory of the virtual Web server where the appropriate is stored
- `page` — name of a page (see later)
- `parameter=value` — name of a parameter and its value (see later). Parameters are optional — if some parameter is not introduced, the default value will be used. Unknown (non-existing) parameter will be ignored. Some pages don't require any parameters.

Note: Lower-case and upper-case letters in page names and parameter names should be preserved. Order of parameters doesn't matter.

All operations will be executed with the rights of anonymous user.

Current Connections

Current connections page can be displayed using the URL:

```
http://netmon:81/conn.html
```

The page doesn't have any configurable parameters.

8.7 Integration of the WWW Interface into the Company Website

Chart of Transferred Data Volume

The following URL displays the page with the chart of transferred data volume:

```
http://netmon:81/chart/form.html
?resolution=1&IP1=1.2.3.4&IP2=5.6.7.8
&IP3=10.11.12.13&service=1
```

where:

- *resolution* — time period from the following table:

<i>Value</i>	<i>Meaning</i>
0	1 minute
1	5 minutes
2	15 minutes
3	1 hours
4	6 hours
5	1 day
6	1 week
7	1 month
8	1 year

- *IP1*, *IP2*, *IP3* — IP addresses for which the transferred data volume will be displayed in the chart (ordered red, green, blue). Instead of an IP address of a particular computer, the address 0.0.0.0 (sum of data volume for all computers) or 127.0.0.1 (loopback address; it will be replaced by the IP address of the computer, where the page was opened) can be entered.
- *service* — monitored service:

<i>Value</i>	0	1	2	3	4	5	6	7
<i>Meaning</i>	All services	HTTP	POP3	SMTP	FTP	Telnet	IMAP4	SSH

If the user wants to display an isolated chart (picture), he can use the following URL:

```
http://netmon:81/chart/image.png
```

All parameters described above remain valid.

Example:

Chapter 8 Web Interface

```
http://netmon:81/chart/image.png
?resolution=3&IP1=0.0.0.0&IP2=127.0.0.1&service=1
```

This example shows an isolated chart for time period 1 hour, the transferred data volume for all computers will be highlighted in red color. The green color will represent the computer used for page viewing.

Table of Transferred Data Volume

The following URL shows the table of transferred data volume (*Report*) according to the specified parameters:

```
http://netmon:81/report/output.html
?interval=2&back=7&columnscout=7&columnwidth=1
&sort=3&direction=3&service=0,
```

where:

- `interval` — basis of column width, it is multiplied by the parameter `columnwidth`. The possible values are:

<i>Value</i>	0	1	2	3	4	5
<i>Meaning</i>	minutes	hours	days	weeks	months	years

- `back` — the beginning of the table will be moved “backwards” by the specified number of time periods. Value 0 means current time.
- `columnscout` — number of columns in the table
- `columnwidth` — width of column. This parameter multiplied by the `interval` parameter determines time interval covered by one column.
- `sort` — table will be sorted by this value:

<i>Value</i>	1	2	3
<i>Meaning</i>	IP address	computer name	transferred data volume

- `direction` — table will display data in this direction:

8.7 Integration of the WWW Interface into the Company Website

<i>Value</i>	1	2	3
<i>Meaning</i>	incoming (download)	outgoing (upload)	sum of both directions

- *service* — data volume will be displayed for this services (see above — section *Chart of transferred data volume*)

Correct parameters settings will be demonstrated at the example.

```
http://netmon:81/report/output.html
?interval=2&back=1&columnscout=7
&columnswidth=1&sort=3&direction=3&service=0
```

- *interval=2* — basis of column width will be one day
- *columnswidth=1* — column width (time period) will be 1 day
- *columnscout=7* — number of columns in table will be 7, the entire table will cover time period of 7 days (1 week)
- *back=1* — table moved backwards by one time period (i.e. 1 week). As a result, the table will cover time period “-2 weeks to -1 week”.
- *direction=3* — table will contain sum of incoming and outgoing data
- *service=0* — total volume of transferred data will be displayed (for all services)

Logs

Logs can be displayed using the URL:

```
http://netmon:81/log/output.html
?log=2&age=7&maxlines=1000&filter=text
```

where:

- *log* — log file number according to the following table:

<i>Value</i>	2	3	4
<i>Meaning</i>	HTTP Log	Connection Log	Mail Log

- *age* — maximum age of log (in days)
- *maxlines* — maximum number of output lines (if more lines satisfy the other conditions, only the most recent lines will be displayed)
- *filter* — text to be searched. Only the lines containing this text will be displayed.

Chapter 9

Glossary of Terms

E-mail address Determines message recipient and sender during communication using the electronic mail.

HTTP Protocol for WWW pages transfer. By default, *TCP* protocol and port *80* is used.

HTTPS Secured version of HTTP protocol. Security is ensured by the encrypted protocol SSL.

By default, *TCP* protocol and port *443* is used.

IMAP Clients can work with their e-mail messages on a server using IMAP. Messages don't need to be downloaded to local computer.

By default, *TCP* protocol and port *143* is used.

Packet Basic communication unit of network layer (i.e. independent of the communication medium). The IP protocol works on packet layer in TCP/IP.

POP3 Post Office Protocol enables users to download e-mail messages from a server to their own local disc.

By default, *TCP* protocol and port *110* is used.

Port A port is a 16-bit number (the allowed range being 1 through 65535) used by TCP and UDP protocols for identification of applications (services) on a particular computer. Several applications may run at once (e.g. WWW server, e-mail client, WWW client — browser, FTP client, etc.). Each application is uniquely determined by its port number. Ports 1 through 65535 are reserved for standard or system use (e.g. 80 = WWW). Ports above 1024 (inclusive) may be used by any application (typically as a source port by a client or by a non-standard server application).

Protocol Format specification of transferred data and methods of their processing. Two computers must use the same protocols to be able to communicate.

Majority of network protocols is standardized, so they can be used for a communication between devices from different vendors. Set of protocols used in the Internet and known in general as TCP/IP can be used as an example.

Chapter 9 Glossary of Terms

Proxy server An older method of Internet connection sharing. Client in a local network does not communicate directly with the target computer in the Internet but it passes its request to a proxy server. The proxy server will process the request and deliver the response.

SMTP Basic protocol used for e-mail delivery in the Internet. Sender and recipient are identified by an e-mail address.

By default, *TCP* protocol and port 25 is used.

Service In network terminology, application used in an network environment is called a service. In TCP/IP, the service is identified by a transport protocol and port (e.g. HTTP uses *TCP* protocol and port 80).

SSL Protocol for secured and encrypted TCP connection. Originally, it was created to secure the transmission of WWW pages by the HTTP protocol (this protocol is called HTTPS). Today, almost all standard Internet services — SMTP, POP3, IMAP, LDAP, etc. — supports SSL.

Communication starts by the exchange of an encryption key, which is later used for a (symmetrical) encryption of the real data.

TLS Transport Layer Security. SSL successor, de facto SSL version 4.

Chapter 10

Index

- 31
- adapter
 - network 21
- computers
 - groups 44
 - list 42
 - names 43
- connection
 - log 56
 - principle of watching 10
- connections
 - active 61
 - current 46
- Daemon 9, 9, 15, 20
- interface
 - network 23, 51
 - Web 59
 - WWW 35
- IP addresses 23
- IP addresses 9, 12, 17, 26
- log
 - Connection Log 56
 - display on WWW page 61
 - Error Log 57
 - HTTP Log 38, 56
 - Mail Log 57
 - storage time 33
 - storing to file 55
- login
 - to the viewer 19
 - WWW interface 59
- logs
 - location on the disk 11
- protocol 25, 29
 - captured data view 50
 - connection monitoring 49
 - HTTPS 38
 - parameters 34
 - TCP 9
 - UDP 9
- service 25
 - debugging 29
 - definition 27
 - display 54
 - principle of watching 10
- users
 - accounts 29
 - login 19
 - number 17
- viewer 19
- Viewer 9
- viewer 16
- Viewer 41

