DVSINFO

DVSNetmon 1.2
User Manual

Revision 1.2 Feb 2003

© 2002-2003 by DVS Informatics Pvt. Ltd. All rights reserved.
DVSNetmon 1.2 to use with Microsoft Windows 9x, Windows ME, Windows NT, Windows 2000.
Microsoft, Windows 95, Windows 98, W indows ME, Windows NT, Windows 2000 are trademarks of Microsoft Corp.

Limited Warranty

DVS Informatics Pvt. Ltd. warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that DVS Informatics Pvt. Ltd. will, at its option, replace any defective media returned to DVS Informatics Pvt. Ltd. within the warranty period or refund the money you paid for the Software.

DVS Informatics Pvt. Ltd. does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

Information in this manual is furnished for information use only. Its subject to change without notice. DVS Informatics Pvt. Ltd. doesn't take any responsibility or liability for any error or inaccuracies that may appear in this manual.

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL DVS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF DVS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL DVS Informatics Pvt. Ltd. LIABILITY EXCEED THE PUR-CHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

Copyright and License

The software which accompanies this license (the "Software") is the property of DVS Informatics Pvt Ltd and is protected by copyright Law. While DVS Informatics continues to own the Software, you will have rights to use the Software after your acceptance of this license. Your rights and obligations with respect to the use of this Software are as follows:

- You may:
  1) Use one copy of the Software on a single computer;
  2) Make one copy of the Software for archival purposes, or copy the software onto the hard dis k of your computer and retain the original for archival purposes;
  3) Use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- You may not:
  4) copy the documentatio n which accompanies the Software;
  5) sublicense, rent or lease any portion of the Software;
  6) reverse engineer, decompile, disassemble, modify, translate,
  7) Make any attempt to discover the source code of the Software, or create derivative works from the Software; or use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version.

Ordering DVSNetmon

To Purchase DVSNetmon License contact at

DVS Informatics Pvt. Ltd.
31, Electronics complex,
Pardeshipura
Indore MP 452010
INDIA
Email: orders@dvsinfo.com
URL for Online order: www.dvsinfo.com

Technical support

DVS Informatics Pvt. Ltd. Provides technical support as follows.

By Fax at +91-731-272058

By Phone at +01-731-230024, 232405 between 9:00 AM to 5:00 PM (GMT+5.30)

By Email at support@dvsinfo.com

DVS Informatics Pvt. Ltd. provides free support for 1 year after purchase of License at no charge.

Your invaluable suggestion, feedbacks are welcome. Please submit your suggestions, feedbacks, corrections or bug report at FAX or Email mentioned above.

About the Guide

Welcome to DVSNetmon 1.2 for monitoring and analyzing Intranet and Internet Traffic.

This Manual is divided in 3 chapters.

Chapter 1 will give you Introduction and Overview of DVSNetmon. This chapter also contains System Requirements for working with DVSNetmon.

Chapter 2 contains instruction for Installation of DVSNetmon.

Chapter 3 provides you enough information for start working with DVSNetmon.

Table of Contents

List of Figures

Chapter 1

Introduction to DVSNetmon

DVSNetmon software is a simple and robust network monitoring software for monitoring the activities on a LAN and then intelligently analyzing it. This can be used to figure out the congestion in a network, to discover any malicious activities going on the LAN (like some user really getting the network down by heavily pumping the packets), monitoring Internet Traffic etc.

Overview of DVSNetmon

Features

- Can run on Windows 98/95/2000 or Linux based machines. The machine should be attached to the user's Ethernet network.
- Snoops the packet at line rate and stores only the important information in a database.
- Various ways to display the stored information from the database. The results come in form of graphs as well as tabular forms.
- Various kinds of query generated by the software gives the loads in the network by a particular machine, by all machines, by various applications in a network, by various applications within a machine.
- Show online and offline network traffic reports.

Architecture

The network monitoring software is developed in form of two distinct modules - Packet Snooper and Packet Analyzer.

This is designed to have flexibility and scalability in the system. This way, the module doing snooping/sniffing of packets can run on a high performance machine. While the module which analyzes the traffic can run on lower end machine also.

Also, both the modules can run on the same machine or can run on different machines. The modules communicate with each other using ODBC connectivity.

Packet Snooper

This module snoops all the packets going on a physical segment of Ethernet (can be 10 or 100 or 1000 Mbps) LAN. It then stores only the required fields from each Ethernet packet into a database. This database supported in current version is mySQL. The support for other databases will be done in the future releases. The database should provide connectivity to the application programs.

The following fields are extracted from each Ethernet packet by the snooper module and are then stored into the database:

- Source Ethernet Address.

- Destination Ethernet Address.
- Network Protocol type (in Ethernet header).
- Source IP address (if network protocol type in Ethernet header is IP).
- Destination IP address (if network protocol type in Ethernet header is IP).
- Transport Protocol Type (if network protocol type in Ethernet header is IP).
- Source Port Number (if the transport protocol type in IP header is UDP or TCP).
- Destination Port Number (if the transport protocol type in IP header is UDP or TCP).
- Timestamp (indicating when the packet traversed on LAN).

This database is maintained according to each day (24 hours), so that the database size is limited and searching in the database is fast.

Packet Analyzer

This module analyzes the information stored by the packet snooper from the database. This analysis is done based on user input i.e. what does user wants to analyze. User can select to view following things using the analyzer:-

- The total number of bytes transferred by every IP machine in the entire network.
- The total number of bytes transferred by a particular IP machine.
- The application/service level breakup of bandwidth in the entire network. In the network?
- The application/service level breakup of bandwidth within a particular machine.

Analyzer then displays the results in two types of formats - the **On-line Reports** and the **Offline Reports**.

The on-line reports, contains the information about the current load in the network from past configured number of minutes. The result of online report is generated in form of table as well as pie/bar charts.

While the offline reports give the network load for the entire day. The results received by the daily reports can be generated in form of a tabular form or in an ASCII based text file.

Minimum Requirements

Hardware

Pentium 300 MHz. 32 MB RAM, Mouse, Color VGA Monitor running at 800x600 and Network Interface card configured for TCP/IP.

Operating System

DVSNetmon can work on PC running Windows 9x, Windows Millennium Addition, Windows NT and Windows 2000 with Winsock 2.0 compliant TCP/IP on network interface card

Software

- WinpCap Packet Capture Driver (DVSNetmon setup will install it too).
- MySQL database server. (User need to install and configure)

Chapter 2

Installation and Configuration

DVSNetmon can install from either DVSNetmon CD or from Internet. If you are installing DVSNetmon from CD, insert DVSNetmon CD into CD drive and run setup.exe from D:\install\setup.exe (assuming CD drive is D: on your system).

Another way is to download Latest Version of DVSNetmon from www.dvsinfo.com, unzip into temporary directory and run setup.exe.

DVSNetmon always install as Evaluation Version, ***Licensing*** Section contains instruction to bring DVSNetmon into Registered Version.

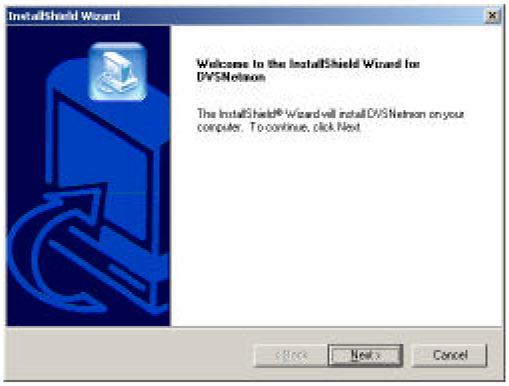
Installation of current version of DVSNetmon doesn't require uninstalling previous version of DVSNetmon.

Installing DVSNetmon in Win9x/NT/2000

If you are installing DVSNetmon in WinNT/2000, make sure you have log on with ***Administrator*** *User Account.*

Installation of DVSNetmon is straightforward. Start installation by double click setup.exe.

Setup will display Welcome screen. Click **Next**

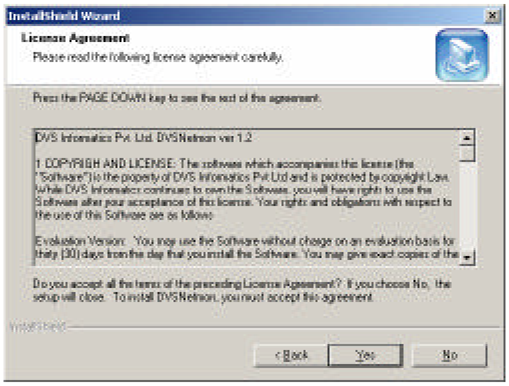


InstallShield Wizard

Welcome to the InstallShield Wizard for DVSNetmon

The InstallShield® Wizard will install DVSNetmon on your computer. To continue, click Next.

Setup will Display Software License Agreement, Click **Yes** to Continue.



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

DVS Informatics Pvt. Ltd. DVSNetmon ver 1.2

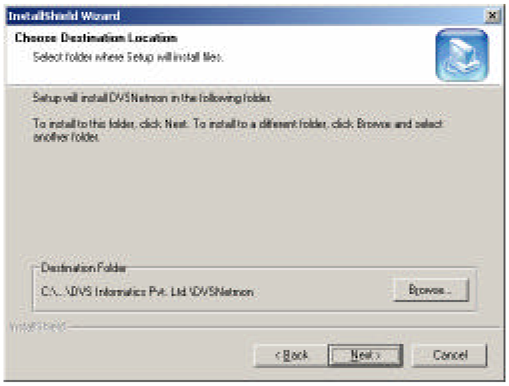
1 COPYRIGH AND LICENSE: The software which accompanies this license (the "Software") is the property of DVS Informatics Pvt Ltd and is protected by copyright Law. While DVS Informatics continues to own the Software, you will have rights to use the Software after your acceptance of this license. Your rights and obligations with respect to the use of this Software are as follows:

Evaluation Version: You may use the Software without charge on an evaluation basis for thirty (30) days from the day that you install the Software. You may give exact copies of the

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install DVSNetmon, you must accept this agreement.

Setup will ask to choose folder, where DVSNetmon will install. Click **Next** after selecting destination folder.

> *If you choose default option, setup will install DVSNetmon in **program files** folder of your windows system.*



Choose Destination Location

Select folder where Setup will install files.

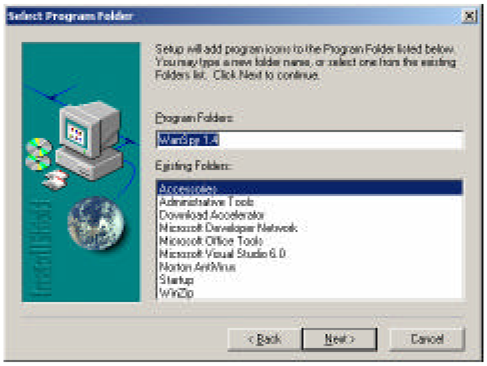
Setup will install DVSNetmon in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\...\DVS Informatics Pvt. Ltd \DVSNetmon

Setup will ask to select Program Group item of Start Menu. Click **Next.**



Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing Folders list. Click Next to continue.

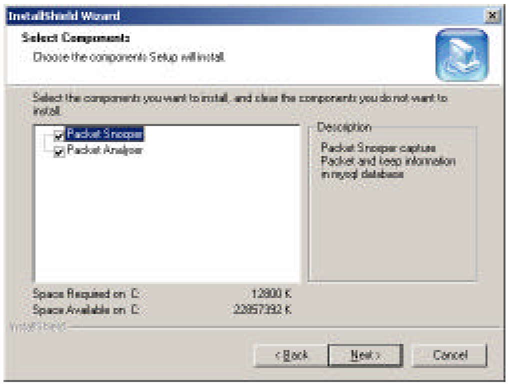
Program Folders:

WanSpy 1.4

Existing Folders:

Accessories
Administrative Tools
Download Accelerator
Microsoft Developer Network
Microsoft Office Tools
Microsoft Visual Studio 6.0
Norton AntiVirus
Startup
WinZip

Setup will ask for type of setup. If you choose Typical or Compact type of setup, it will install all required component of DVSNetmon. If choose custom type of setup you will be able to choose component of DVSNetmon to install.



Choose the components Setup will install.

Select the components you want to install, and clear the components you do not want to install.

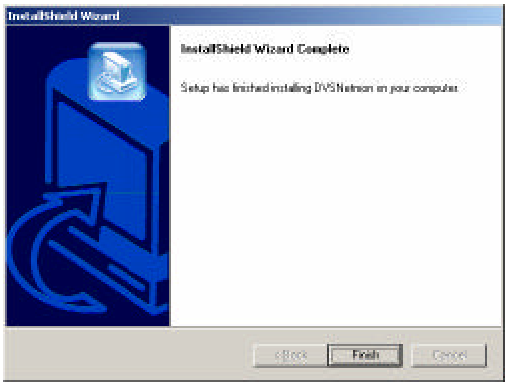
☑ Packet Snooper
☑ Packet Analyzer

Description

Packet Snooper capture Packet and keep information in mysql database

Space Required on C: 12800 K
Space Available on C: 22857392 K

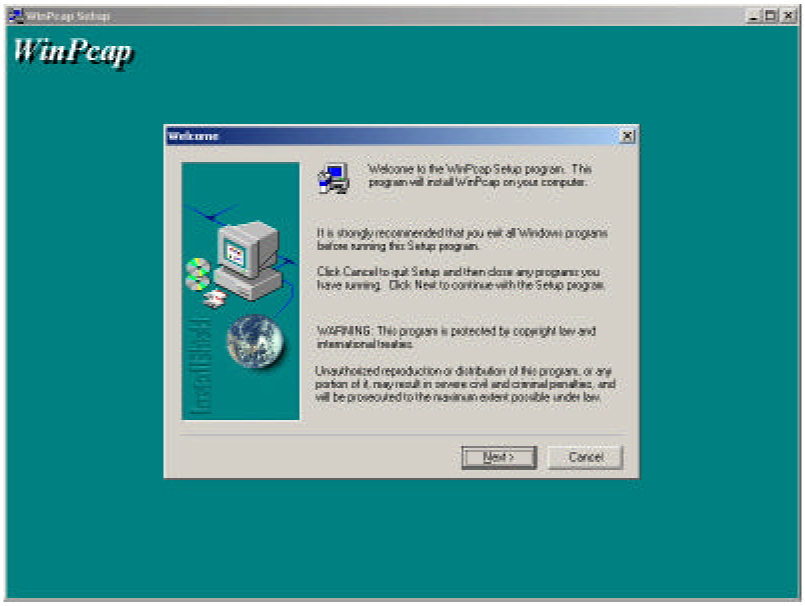
Setup will now copy DVSNetmon files into appropriate folder.



Setup has finished installing DVSNetmon on your computer.

Click Finish.

After installing DVSNetmon, setup will automatically invoke WinPcap Packet Driver installation. Installation of Packet Drier is necessary to run DVSNetmon.



Welcome to the WinPcap Setup program. This program will install WinPcap on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Registering

When DVSNetmon is installed first time on system, it will work for 30 days of evaluation period with full functionality. After that you need to purchase License and Register DVSNetmon.

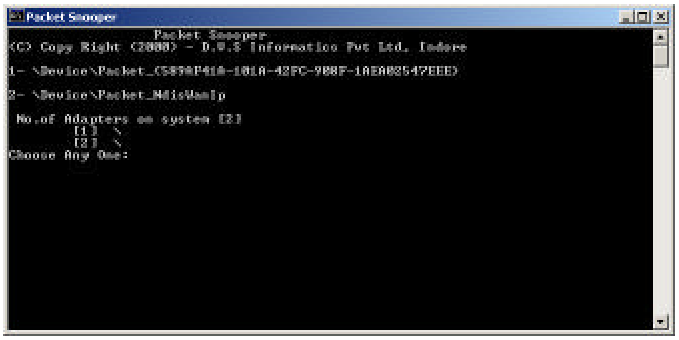
Chapter 3

Working with DVSNetmon

Running Packet Snooper

Packet Snooper of DVSNetmon captures packet on LAN and store information into Mysql database. For viewing online report of Internet and Intranet traffic, Packet Snooper must be started and keep on running. Offline report can be viewed without running Packet Snooper. (See details of Online and Offline report in Later Sections)

Packet Snooper can be launch by clicking Start Menu->Program Files->DVSNetmon->Packet Snooper.



```
                    Packet Snooper
(C) Copy Right (2000) - D.V.S Informatics Pvt Ltd. Indore

1- \Device\Packet_(5890F410-101A-42FC-980F-1AEA02547EEE)

2- \Device\Packet_NdisWanIp

 No.of Adapters on system [2]
        [1 ]  \
        [2 ]  \
Choose Any One:
```

Figure 3-1. Running Snooper

Make sure MySQL Server is running, on same system where you are going to start Packet Snooper.

Packet Snooper will display list of Network Adapters installed on system. Choose Adapter of which you want to capture packets.

After your selection of Adapter, if no error has been occurred snooper starts capturing data until you close it by pressing Ctrl-C.

Running Packet Analyser

Packet Analyser do analysis of packets and display reports and charts of Network traffic. Packet Analyser can be launch by clicking Start->Programs->DVSNetmon->Packet Analyser.

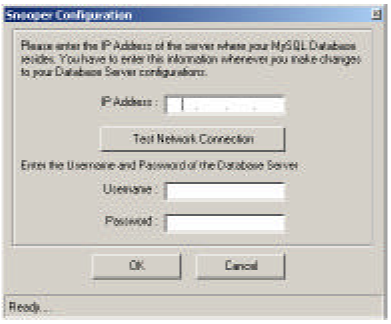
By Default Packet Analyser will try to connect MySQL server at local host (127.0.0.1) with username “dvsinfo” password “dvsinfo”. If you are running MySQL server and Packet Snooper on other system then Packet Analyser will fails to connect to MySQL server with default parameters and will open Snooper Configuration windows.

Make sure MySQL Server is running, before running Packet Analyser.

Configuration

Snooper Configuration

To change default Snooper Configuration Open Snooper Configuration box by clicking on Database->Configure Snooper.



Please enter the IP Address of the server where your MySQL Database resides. You have to enter this information whenever you make changes to your Database Server configurations.

IP Address :

Enter the Username and Password of the Database Server

Username :

Password :

Figure 3-2. Configuring Snooper

IP Address – Give IP Address of server where MySQL server is running and database of Packet Snooper is kept.

Test Network Connection – Check the network connectivity with IP address you entered.

Username: Username of Snooper database at MySQL server.

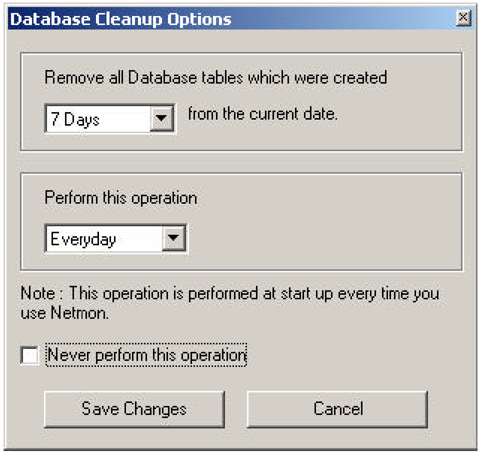
Password: Password of given Username.

Click **OK** button to make configuration into effect.

Same configuration windows will open if Packet Analyser fails to connect with MySQL server.

Database Cleanup Options

Packet Snooper creates everyday a new database for that day. Size of database may be huge depending upon network traffic. Database cleanup feature of Packet Analyser facilitate user to clean database at user specified schedule and save disk space. See later section for cleaning database manually.



Remove all Database tables which were created

7 Days from the current date.

Perform this operation

Everyday

Note : This operation is performed at start up every time you use Netmon.

□ Never perform this operation

Figure 3-3. Database cleanup Options

Never perform this operation – By default this check box is checked and database cleanup feature is disabled. Uncheck this box to enable database cleanup options.

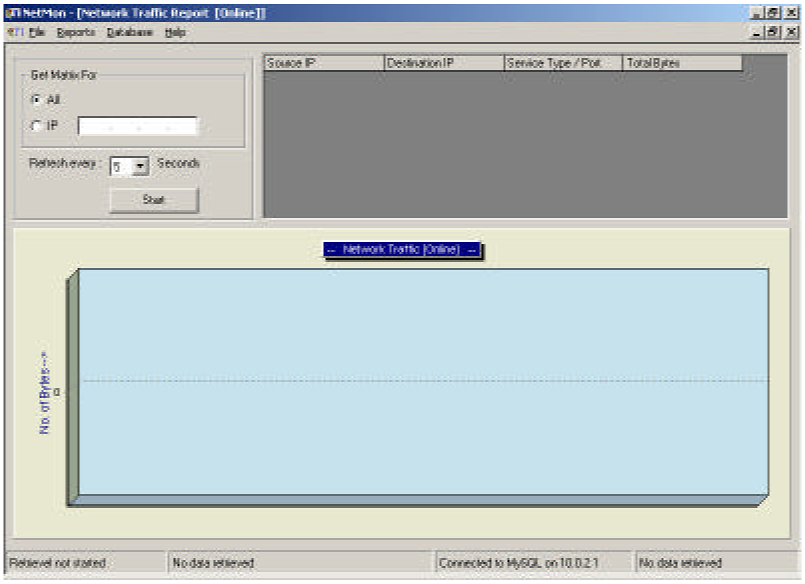
Database Removal – Select Number of days after which database need to clear automatically.

Perform Operation – Select at what time database cleanup option will perform.

Database cleanup operation performs only when Packet Analyser application starts.

Online Intranet Report

Online Intranet Report displays table and charts of current network traffic. Click Reports->Intranet Report (Online).


NetMon - [Network Traffic Report [Online]]
File
Reports
Database
Help
Start
-- Network Traffic [Online] --
No. of Bytes-->
0

Get Matix For
● All
○ IP

Refresh every : 5 Seconds

Source IP	Destination IP	Service Type / Port	Total Bytes

Retrieval not started | No data retrieved | Connected to MySQL on 10.0.2.1 | No data retrieved

Figure 3-4. Online Intranet Report

Default selection of **"All"** will display report of while network traffic. To view report of particular IP address, select **"IP"** and enter IP address.

Refresh Rate is time interval after that Analyser refresh table and chart of network traffic.

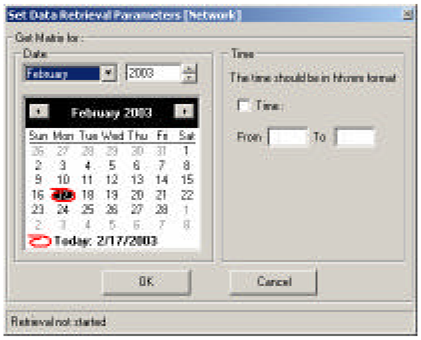
Online report refreshes report and chart every refresh rate seconds. It's recommended that if you are viewing online report, run Packet Analyser on same system where Packet Snooper and MySQL server is running.

Online Internet Report

Online Internet Report show current network traffic between host on your local Network and any host on Internet or outside of your Intranet. Click Reports->Internet Report (Online).

Offline Intranet Report

You can display Network Traffic report of past days, week or month. To open offline Intranet report click on Reports->Intranet Report (Offline).



Set Data Retrieval Parameters [Network]

Get Matrix for :

Date: February 2003

The time should be in hh:mm format

□ Time:

From: To:

Today: 2/17/2003

Retrieval not started

Figure 3-5. Date selection

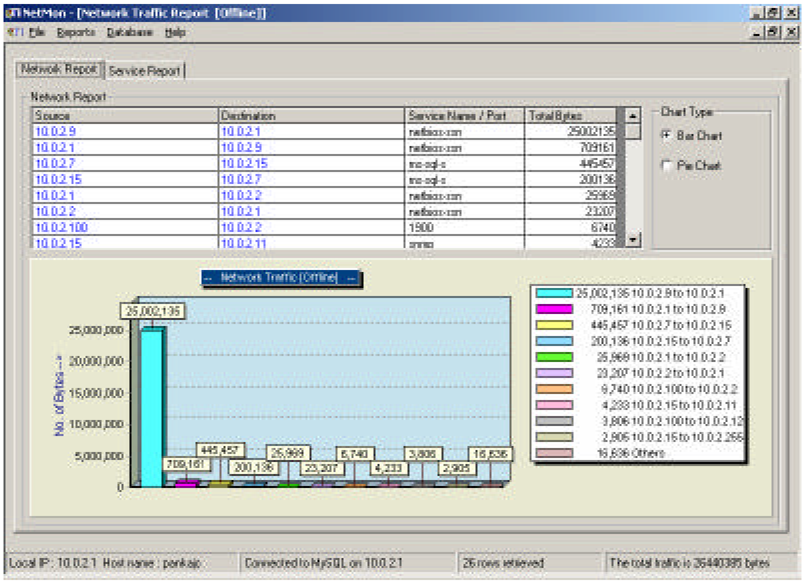
Select data of which you want to see report. By default report of whole day will display otherwise you can enter time period too after check "**Time**" check box.

Press **OK**, it will take some time to generate report.

It is require that, Snooper was running on selected data and time.

Network Report

In Network Tab of Intranet report windows, Traffic report between two hosts IP of your local network for well known services will display.



NetMon - [Network Traffic Report [Offline]]

Network Report

Source	Destination	Service Name / Port	Total Bytes
10.0.2.9	10.0.2.1	netbios-ssn	25002135
10.0.2.1	10.0.2.9	netbios-ssn	709161
10.0.2.7	10.0.2.15	ms-sql-s	445457
10.0.2.15	10.0.2.7	ms-sql-s	200136
10.0.2.1	10.0.2.2	netbios-ssn	25969
10.0.2.2	10.0.2.1	netbios-ssn	23207
10.0.2.100	10.0.2.2	1900	6740
10.0.2.15	10.0.2.11	snmp	4233

Chart Type: ● Bar Chart ○ Pie Chart

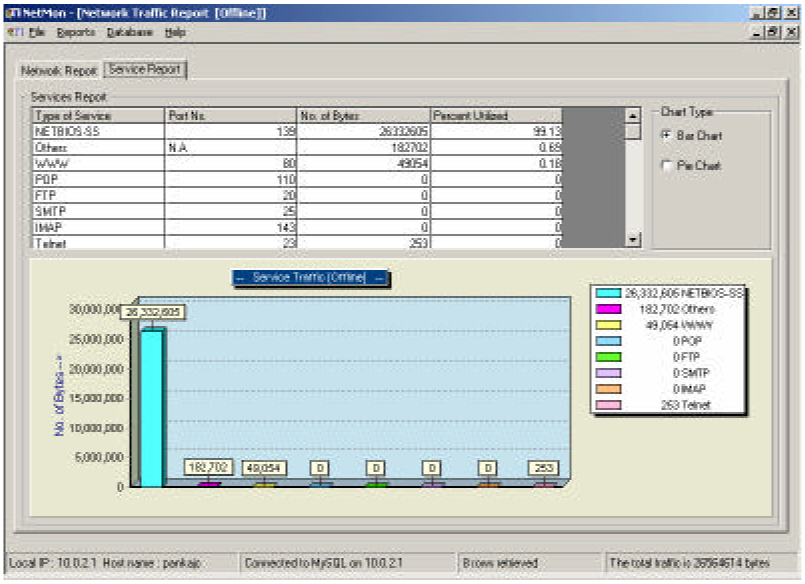
Local IP : 10.0.2.1 Host name : pankaj | Connected to MySQL on 10.0.2.1 | 26 rows retrieved | The total traffic is 26440385 bytes

File
Reports
Database
Help
Network Report
Service Report
-- Network Traffic [Offline] --
No. of Bytes -->
25,000,000
20,000,000
15,000,000
10,000,000
5,000,000
0
25,002,135
709,161
445,457
200,136
25,969
23,207
6,740
4,233
3,806
2,905
16,636
25,002,135 10.0.2.9 to 10.0.2.1
709,161 10.0.2.1 to 10.0.2.9
445,457 10.0.2.7 to 10.0.2.15
200,136 10.0.2.15 to 10.0.2.7
25,969 10.0.2.1 to 10.0.2.2
23,207 10.0.2.2 to 10.0.2.1
9,740 10.0.2.100 to 10.0.2.2
4,233 10.0.2.15 to 10.0.2.11
3,806 10.0.2.100 to 10.0.2.12
2,905 10.0.2.15 to 10.0.2.255
16,636 Others

Figure 3-6. Offline Intranet Report (Network)

Service Report

In Service Report tab, data transferred of well know services will display.



Type of Service	Port No.	No. of Bytes	Percent Utilized
NETBIOS-SS	139	26332605	99.13
Others	N.A.	182702	0.69
WWW	80	49054	0.18
POP	110	0	0
FTP	20	0	0
SMTP	25	0	0
IMAP	143	0	0
Telnet	23	253	0

Local IP : 10.0.2.1 Host name : pankajc | Connected to MySQL on 10.0.2.1 | 8 rows retrieved | The total traffic is 26564614 bytes

Figure 3-7. Offline Intranet Report (Services)

To save table or graph click on File->Save->table/graph menu.

Same way table or graph can be print by clicking on File->Print->table/graph menu.

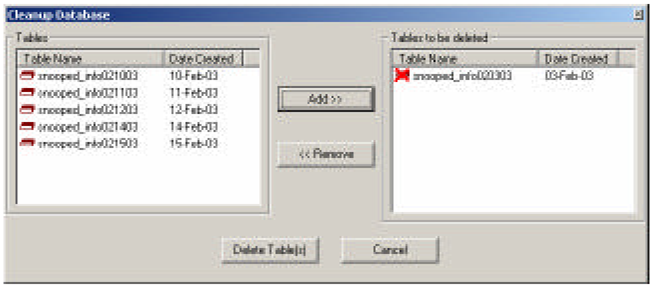
Offline Internet Report

Like Offline Intranet Report, Offline Internet Report shows traffic of past days, week or month between local network and Internet.

Click on Report -> Internet Report (offline) to open offline internet report.

Cleanup Database Manually

In addition to automatically cleaning database created by Packet Snooper, database which is not required can be deleting manually.



Tables

Table Name	Date Created
snooped_info021003	10-Feb-03
snooped_info021103	11-Feb-03
snooped_info021203	12-Feb-03
snooped_info021403	14-Feb-03
snooped_info021503	15-Feb-03

Tables to be deleted

Table Name	Date Created
snooped_info020303	03-Feb-03

Figure 3-8. Manually clean database

In right panel list of all available database will display, select database you want to delete and clock on **Add>>**. After adding all databases you want to delete, click on **Delete Table(s).**