

Distinct[®]

Network Monitor[™]

Version 4.2

User's Guide

Distinct Corporation

3315 Almaden Expressway
San Jose, CA 95118 USA

Phone: +1 408-445-3270
Fax: +1 408-445-3274

Email: sales@distinct.com

WWW: <http://www.distinct.com>

Disclaimer

Distinct Corporation makes no warranties as to the contents of this documentation and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Information in this manual is subject to change without notice and does not represent a commitment on the part of Distinct Corporation. The Software described in this manual is furnished under a license agreement and may be used or copied only in accordance with the terms of that agreement.

Copyright Notice

© 1997 - 2003 by Distinct Corporation All rights reserved.

No part of this publication may be reproduced, transmitted or translated into any language by any means without the express written permission of Distinct Corporation.

Trademarks

Distinct is a registered trademark and Network Monitor is a trademark of Distinct Corporation. Windows and Microsoft Excel are registered trademarks of Microsoft Corporation. Other product names are trademarks or registered trademarks of their respective owners.

April 11th, 2003

Published in the United States of America

1 - INTRODUCTION.....	1
OVERVIEW	1
<i>Packet Analyzer</i>	1
<i>Network Segment Traffic Statistics</i>	1
INSTALLING NETWORK MONITOR	2
System Requirements	2
Installation	2
Activating the Network Monitor License	2
<i>Installing a Network Monitor Agent</i>	3
Changing the Agent's Configuration	3
Encrypting packets.....	3
Uninstalling Network Monitor.....	3
<i>About this Manual</i>	3
2 – GETTING STARTED.....	4
TAKING A NETWORK CAPTURE	4
<i>Defining your Capture Settings</i>	4
<i>Defining your Statistics Settings</i>	7
Report Folder.....	7
Bandwidth Settings.....	7
Chart Type.....	7
Chart Settings	8
Show Statistics.....	8
3 - NETWORK MONITOR AGENTS	9
<i>Configuring Agents from Network Monitor</i>	9
Starting a Capture or Statistics on an Agent	11
4 - USING FILTERS	12
Creating a Filter with the built-in Templates	12
Creating a Basic Filter Using Advanced Expressions.....	14
Creating Advanced Filters with Advanced Expressions	15
Applying a Filter to the Capture	18
Applying a Filter to an Existing Capture File	18
Managing your Filters.....	19
5 - VIEWING YOUR CAPTURE FILE.....	20
<i>Customizing the way you View a Capture File</i>	20
<i>Ports and Captured Packets</i>	23
Searching a Capture File.....	23
Saving Parts of a Capture File with Another Name	23
<i>Modifying and Resending Captured Packets</i>	24
6- VIEWING YOUR STATISTICS FILE.....	25
<i>All IP Traffic</i>	25
Whols	26
<i>Application Protocols</i>	26
<i>Network Protocols</i>	27
<i>IP Protocols</i>	27
<i>MAC Traffic</i>	27
<i>Bandwidth</i>	28
<i>Packet Sizes</i>	28
<i>Adapter Statistics</i>	29
General Statistics	29
Ethernet Statistics	30
<i>Summary</i>	30
CREATING REPORTS	31

7 – IMPORTING AND EXPORTING	32
<i>Converting Third Party Capture Files</i>	<i>32</i>
<i>Saving a Packet Capture to a Text File</i>	<i>32</i>
8 – PRINTING A CAPTURE FILE.....	34
<i>Setting your Print Options.....</i>	<i>34</i>
<i>Printing a Capture File</i>	<i>34</i>
9 – OTHER TOOLS.....	35
<i>Ping</i>	<i>35</i>
<i>TraceRoute</i>	<i>35</i>
<i>WhoIs.....</i>	<i>35</i>
<i>TCP and UDP Connections.....</i>	<i>35</i>
<i>Scan TCP Ports</i>	<i>36</i>
<i>Base Conversion.....</i>	<i>36</i>

1 - Introduction

Overview

The Distinct Network Monitor captures network traffic and translates the protocol negotiation of that traffic into simple English. It is the perfect solution for understanding the type of network traffic that is going over the network as well as for pinpointing network related problems. It is a must for both software developers who write applications that will work over a network as well as for MIS personnel who are trying to diagnose network related problems and bottlenecks.

Packet Analyzer

What is essentially different between a plain packet sniffing product and Distinct Network Monitor is that the Distinct Network Monitor interprets the packets for any specific connection and is able to pinpoint any errors it sees by marking these with a black X. Some packets are marked with a white X; these do not necessarily denote an error but are a warning of packet retransmission and other non-fatal network errors.

Distinct Network Monitor can capture the traffic that is on the subnet or on the switch segment in case of a switched network as long as the network interface card installed in the computer that is running the monitor is able to run in promiscuous mode.

Network Segment Traffic Statistics

Distinct Network Monitor is able to capture and display network traffic statistics for the network segment it is capturing on. As with the packet-analyzing feature of this product, statistics are restricted to the network segment or segments being monitored. With the help of Network Monitor Agents, the Network Monitor may view statistics from various network segments concurrently. The statistics captured and displayed are the following:

- The list of IP addresses that are active on the network segment, showing the total number of bytes sent and received by each IP address.
The type of IP address is shown. This may be L for an IP address on the local network, B for a broadcast address, or M for multicast addresses.
Note that if the system listed is not on the same hub, the traffic numbers do not indicate the total traffic for that system, but just the traffic created between it and other systems on the hub or switch being monitored. Details of the packet distribution per protocol are also given for each IP address in the list.
- The list of application protocols showing how many bytes were sent and received for each protocol. Protocols are identified by port number. It also shows which IP addresses generated the traffic.
- The list of IP protocols and the total number of bytes and packets transmitted for each one.
- The list of level three protocols such as IP and Netbeui showing the total number of bytes and packets transmitted for each one.

- Bandwidth usage over the specified time period using the number of samples specified.
- The list of MAC addresses that are active on the network segment. The total number of packets and bytes that were sent and received by each MAC address. This includes all packets whether IP or otherwise that are over Ethernet or Token Ring and may include packets that are not parsed by the Network Monitor.
- Analysis of Packet size distribution showing the number of packets transmitted in various size ranges.
- Summary of the statistics recorded during the session.

All these statistics are automatically gathered and displayed in a window alongside the Capture window each time a capture is started. If you need to gather statistics for one or more segments you may run statistics only without taking the network trace, which would require too many resources if run over several hours. This allows you to monitor systems over several hours without the need to save all the packets that are traveling on the wire.

Installing Network Monitor

Before you install Distinct Network Monitor, make sure that the system you will install on has adequate disk space to save the capture files. Depending on the volume of traffic, non-filtered capture files can be very large. There are more network packets traveling on your network segment than you may imagine. Network Monitor will perform best on systems with fast hard disks and that have plenty of memory.

System Requirements

The minimum requirements are a Pentium 500 MHz system with 128 MB RAM and adequate hard disk space. The recommended system is a 800 MHz or higher system with 256 MB or more of RAM and adequate disk space. If you intend to run the monitor over 24 hour periods or more to capture all packets at a router, it is advisable to have additional memory on the system doing the capture.

Installation

To install Network Monitor simply run **network-monitor.exe** and follow all the instructions as they appear on the screen.

Installation of Network Monitor requires Administrator privileges on NT, 2000 and XP systems.

Activating the Network Monitor License

Before you can use a licensed copy of Network Monitor you must register it at the Distinct Web site to obtain the key code to be entered. When you purchased the product you received a serial number and product identification number. Both of these are needed to register your copy. When you have your key code, you will need to enter this together with the serial number in the Distinct License Manager box that is displayed when you run Network Monitor for the first time. If you have upgraded your monitor to use multiple Agents, you need to enter the new serial number in the Update License box in the Help menu.

Installing a Network Monitor Agent

To install the Distinct Network Monitor Agent run the **DNMAgent.exe** on the system you wish to install on. The installation process requires you to configure the Agent. The following items need to be configured:

- You need to specify the port that the Agent will listen on. The default port is port 9999, which is a port that is reserved for Distinct Corporation. Note that if you intend to access this agent across a firewall, you will need to open the selected port on the firewall.
- You are also required to set a password for the agent. This password will be required to monitor the agent from the Network Monitor. If you have multiple agents it may be convenient to keep a single password for all agents. This is however not required.

After installation the Agent is automatically started and its icon will appear on the system tray. This means that the agent is ready and the system can now be monitored using Network Monitor. The Agent is closed by right clicking its icon and selecting Exit.

Changing the Agent's Configuration

You may modify the Agent's listening port, password or connection timeout by clicking the Agent's icon and selecting the button corresponding to the parameter to be changed. The connection timeout sets the amount of time that the Agent will wait for a request from a Network Monitor that has connected to it but made no specific request, such as listing adapters or starting a capture. Once the Agent is connected to a Network Monitor, no other connection may be made to the listening port until Network Monitor terminates the connection or it has timed out and disconnected automatically.

Masking Strings

Users on the Agent systems may be asked to enter passwords and other critical information in the Mask string(s) text box. Multiple entries should be space, comma or semi-colon delimited. Strings entered here will automatically be replaced by xx in the actual trace taken.

Encrypting packets

The packets captured will traverse the network. Therefore, if security is an issue it is a good idea to select the Encrypt packets option. Note however, that turning encryption on will slow down the whole process, as all packets will need to be encrypted by the Agent and then decrypted by the Network Monitor.

Uninstalling Network Monitor

To uninstall Network Monitor you must use the Uninstall program by calling it from the Add/Remove Programs group in Control Panel.

About this Manual

This manual is intended as a User's Guide. It is not a reference manual. For help on a particular menu item please use the on-line context sensitive help in the product.

2 – Getting Started

Taking a Network Capture

With Distinct Network Monitor you can choose to capture all the packets and statistics that are visible to your NIC driver or just the statistics. If you are only interested in gathering the statistics that will show you the statistics breakdown of IP addresses and protocols, rather than analyzing individual packets, choose only to capture statistics. The capture of packets should be used if you need to analyze the network traffic and are specifically looking for protocol errors or other problems.

To start your first network capture of packets and statistics click on the double triangle button in the toolbar. To start a capture of statistics only click the pink triangle button next to it. To start a capture of packets only, click on the green triangle button. The first time you start a capture, the Capture Settings dialog box is displayed allowing you to choose the folder in which to save the capture files and set other parameters. To stop the capture, click on the red square in the toolbar.

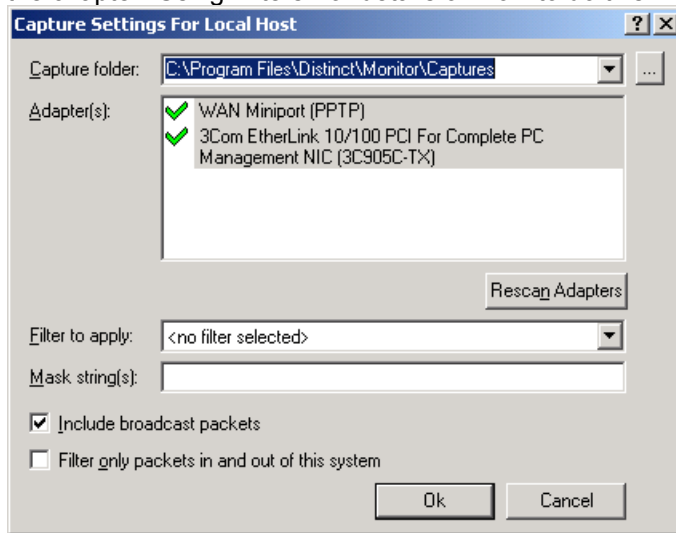
Note that when you are capturing both the packets and statistics you can toggle between each of these by clicking on the tabs at the bottom of the window.

Defining your Capture Settings

The first time you run Distinct Network Monitor you need to define your capture settings for your local host. A dialog box will automatically be displayed for you to do this. You can later modify these settings by selecting **Capture Settings** in the **Configure** menu.

1. Enter the complete path of the folder in which you wish the capture file to be created or use the Browse button to locate it. Note that Network Monitor will remember the last capture setting saved for each folder.
2. If your system has more than one adapter, you may select the adapter or adapters from which you wish to record the network traffic. By default Network Monitor will capture the traffic from all the adapters on your system.
3. If you wish to only save the traffic related to specific protocols, select the appropriate filter from **Filter to Apply**. Before you can select a filter you will need to create it. See

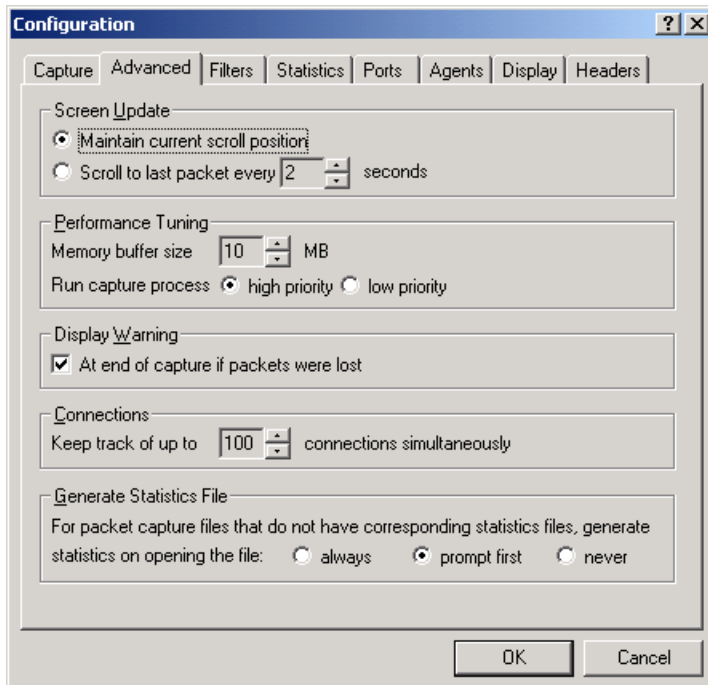
the chapter “Using Filters” for details on how to do this.



4. You may also choose to mask certain information from the actual capture. For example, if you know that to reproduce an error you are trying to diagnose you must access a certain database record that would display a social security number, you could enter that number here and the actual capture will mask the information allowing you to get help without giving out any sensitive information to other engineers helping you. Passwords may also be masked in this way. Multiple entries should be space, comma or semi-colon delimited. All entries are case sensitive.
5. You may also include or exclude broadcast packets from your capture.
6. You may select to capture only those packets that are sent and received from the system running Network Monitor, thus ignoring all other packets on the subnet.
7. Click **OK** to save your settings.

Fine Tuning Driver Capture Settings

To optimize performance of your Network Monitor driver you may fine-tune the Capture Settings. To do this, select the **Advanced** option from the **Configure** menu. This displays the Advanced Capture Settings tab. Here you can fine-tune the screen update, performance and display parameters.



Screen Update

The screen update options allow you to decide how the screen should be updated during a network packet capture. You have two choices:

- Maintain your current scroll position. If you intend to scroll through the capture while it is going, it is probably best to select **Maintain current scroll position**. This means that the packets currently displayed will remain displayed even though the capture is going on and more packets are being added.
- Scroll to the last packet at the specified interval. If on the other hand you prefer to watch the packets as they are being captured you should select the option to Scroll to the last packet every few seconds. Two seconds will work for most systems, however, you can choose to make this faster or slower as needed to minimize the flickering that automatic scrolling causes.

Performance Tuning

Depending on the memory available on your system you will want allocate more or less of your available memory to the capture buffer. Larger buffers may be more efficient on more powerful systems. Whenever you experience packet loss in a capture, it is a good idea to try increasing this value (within the limits of the available memory on your system) for better performance.

You may also choose to run the capture as a high or low priority process on the system. For best performance, run it as high priority.

Display Warning

At the end of each capture, you may choose to display a warning if the capture driver lost any packets during the capture.

Connections

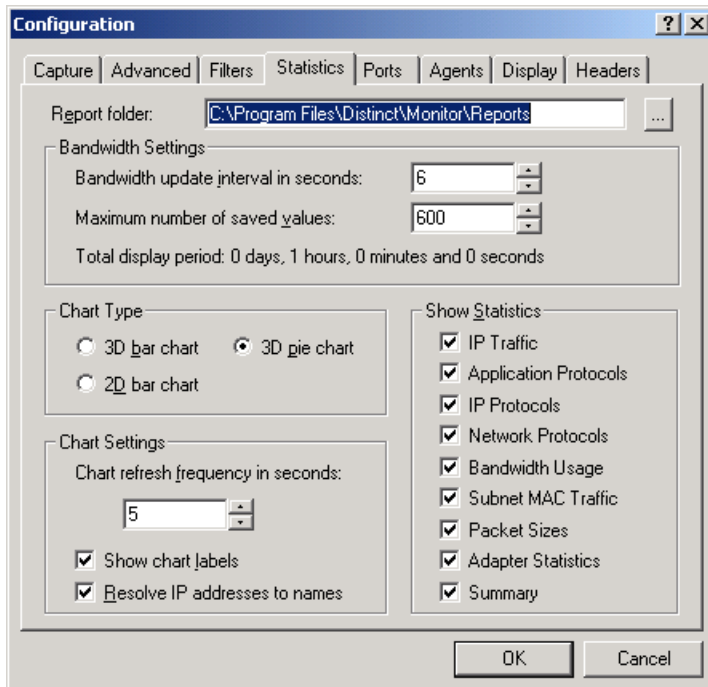
This option allows you to decide how many connections Distinct Network Monitor will show as a single connection. When a packet is right clicked and **Display only packets of this connection** is selected, the window will display only packets of that specific connection. However, if the particular trace contains more than 64 connections, packets from more than one connection may be present. You may increase this number as required.

Generate Statistics File

When a packet capture has been taken without also capturing the statistics, it is possible to generate the statistics for that capture at a later time. Here you can choose to be prompted to create the file, to have that file created automatically, or to never generate statistics for packet capture files when opening them. Note that Adapter statistics will not be generated when generating the statistics file this way.

Defining your Statistics Settings

Several statistics settings can be configured through the Statistics Settings Configuration tab. Here you can decide which statistics should be viewed and how you wish to view them.



Report Folder

This is the folder in which all the Statistics reports you generate will be saved to. See the section Creating Reports, in this manual for more information on what Statistics reports can be created.

Bandwidth Settings

The bandwidth settings allow you to map the period of time you wish to see bandwidth statistics for and decide the number of values to save. For example if you wished to monitor the bandwidth over one day taking 5 minute intervals, you would set both the bandwidth update interval and the maximum number of saved values to 300. Reducing the update interval and increasing the maximum number of saved values may slow down the system.

Chart Type

Here you can decide how you wish to view your charts. You can have a three-dimensional bar chart, a three-dimensional pie chart or a two-dimensional bar chart.

Chart Settings

You can modify the refresh rate of the statistics charts. If you are experiencing any type of performance slow down, you may try to increase this value.

You may also choose to show chart labels by checking the **Show chart labels** option.

The Network Monitor will try to resolve all IP addresses to host names. This requires DNS lookup. If DNS is not defined on your system you must turn the **Resolve IP addresses to names** feature off.

Show Statistics

Here you can select which Statistics charts are to be displayed. Building and maintaining the Bandwidth charts requires a higher memory usage. If the system is experiencing any type of slowdown, you may try turning off the Bandwidth if you are not interested in these statistics.

3 - Network Monitor Agents

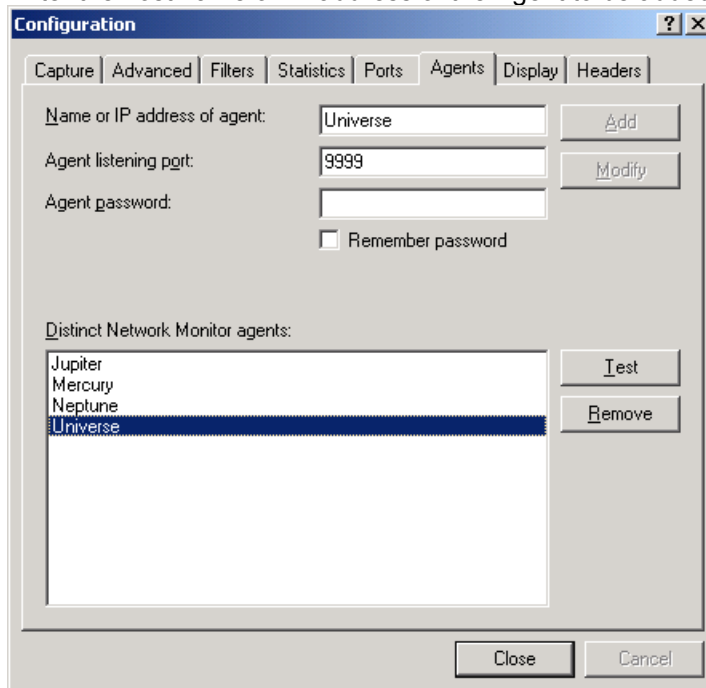
Distinct Network Monitor may be set up to monitor remote Agents. The Network Monitor license comes with one Agent and additional Agents may be purchased and deployed as needed.

Once the Agents have been installed, you need to define and configure them before they can be started. The port to listen on and the password must be set. The mask string(s) may also be set at the Agent. Before starting the capture some configuration needs to be done for each Agent from the Network Monitor.

Configuring Agents from Network Monitor

Before an Agent can be configured it must be defined as an Agent to which access will be allowed by the Network Monitor. To do this select **Agents** from the **Configure** menu. Then:

1. Enter the host name or IP address of the Agent to be added in the name field.

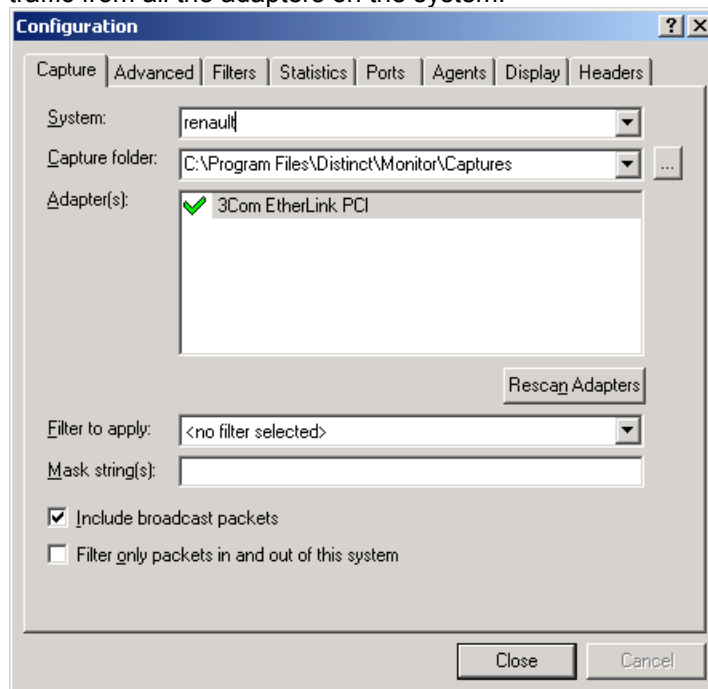


2. By default each Agent will listen on port 9999 for instructions from an authorized Network Monitor. Port 9999 is a well-known port that is assigned to Distinct Corporation and should therefore not be in use by other applications. If you have set up the Agent to listen on a different port you must enter that port number here. The password used must also be the same password that was used to configure the Agent.
3. You may test the connection by selecting the Agent's name in the Distinct Network Monitor Agents list box and clicking the Test button. This will attempt to connect to the Agent to see if it is up and running.

Defining Capture Settings for an Agent

Before you can start a Capture or statistics on an Agent you must define its Capture Settings directly from the Network Monitor (if you do not do this the system will automatically prompt you to do so the first time around). Once you have added the Agents through the Agents Configuration tab, you are now ready to configure them by selecting Capture Settings from the Configuration menu.

1. Select the Agent to be configured in the System pull down list box. If you have not saved the password on your system for this agent, you will be asked to enter the password. Note that this is the password that was given when the Agent was installed.
2. Enter the complete path of the folder in which you wish the capture file to be created or use the Browse button to locate it. Note that Network Monitor will remember the last capture setting saved for each folder.
3. If the system has more than one adapter you may select the adapter or adapters from which you wish to record the network traffic. By default Network Monitor will capture the traffic from all the adapters on the system.



4. If you wish to only save the traffic related to specific protocols or that meets the criteria specified by any filter you have created, select the appropriate filter from **Filter to apply**. Before you can select a filter you will need to create it. See the chapter "Using Filters" for details on how to do this.
5. You may also choose to mask certain information from the actual capture. For example, if you know that to reproduce an error you are trying to diagnose you must access a certain database record that would display a social security number, you could enter that number here and the actual capture will mask the information allowing you to get help without giving out any sensitive information to other engineers helping you. Passwords may also be masked in this way. You may have more than one entry. Entries should be space, comma or semi-colon delimited. All entries are case sensitive.
6. You may also include or exclude broadcast packets from your capture.

7. You may select to capture only those packets that are sent and received from the system running Network Monitor, thus ignoring all other packets on the subnet.
8. Click **Close** to save your settings.

Starting a Capture or Statistics on an Agent

Remote Agents can capture both Packets and Statistics or just the statistics.

Capturing Packets on an Agent

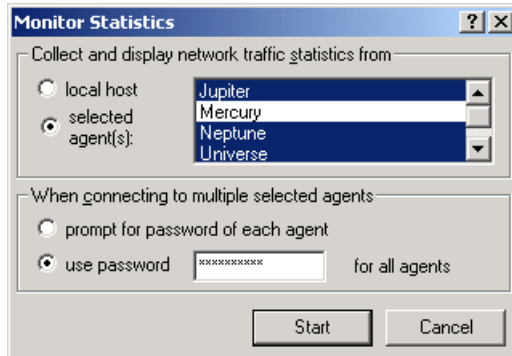
To capture and analyze packet from a remote Agent you must first configure the Agent as described above then click the little triangle button to start the capture. Both the packets and statistics will be captured. Network Monitor can capture packets from one remote Agent at a time.

Capturing Statistics on an Agent

Distinct Network Monitor allows you to capture Statistics from multiple Agents at the same time. The results may be displayed in individual windows, one per Agent.

To start the Statistics capture:

1. Select the **Statistics** command from the **Capture** menu or click the statistics button in the

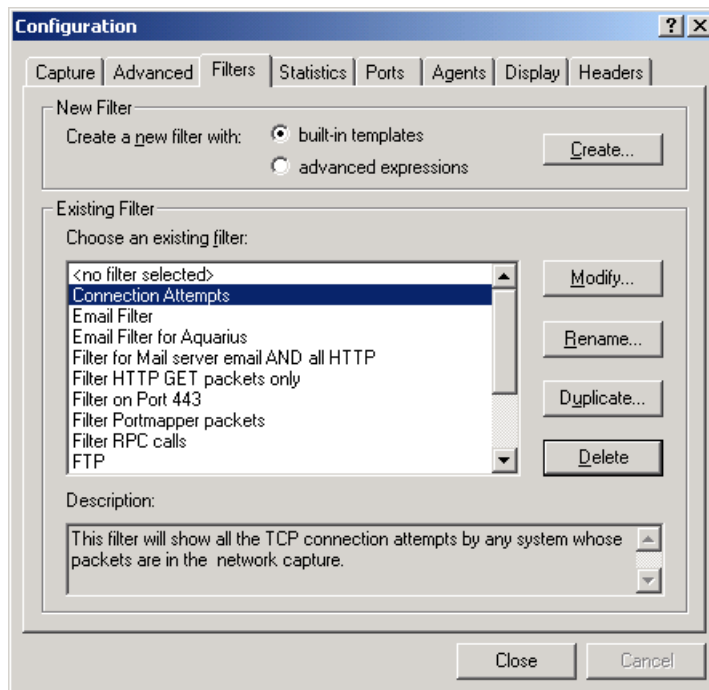


menu bar.

2. Choose the Selected Agent(s) radio button. Then select the Agents you wish to monitor from the list box.
3. If you have not saved the password for each Agent on your local system, you will need to provide the password to connect to each Agent before it can be started. If you are using a single password for all Agents in question select the Use Password radio button and enter the password and port to be used for the connection to all Agents. If you are using different passwords for each Agent, you will need to enter all the passwords one at a time before you can connect to the Agents.

4 - Using Filters

Distinct Network Monitor allows you to create and set powerful filters. You may set a filter for the capture itself to actually save only the filtered packets to a file. You may also apply a filter to a previously saved capture file to view only the filtered packets from that file. Whichever method of filtering you use, you must first create your packet filters. The Distinct Network Monitor is shipped with some Filter examples as well as built-in templates for most filtering needs. Filter configuration management is done through the Filters tab, which you select from the **Configure** menu.

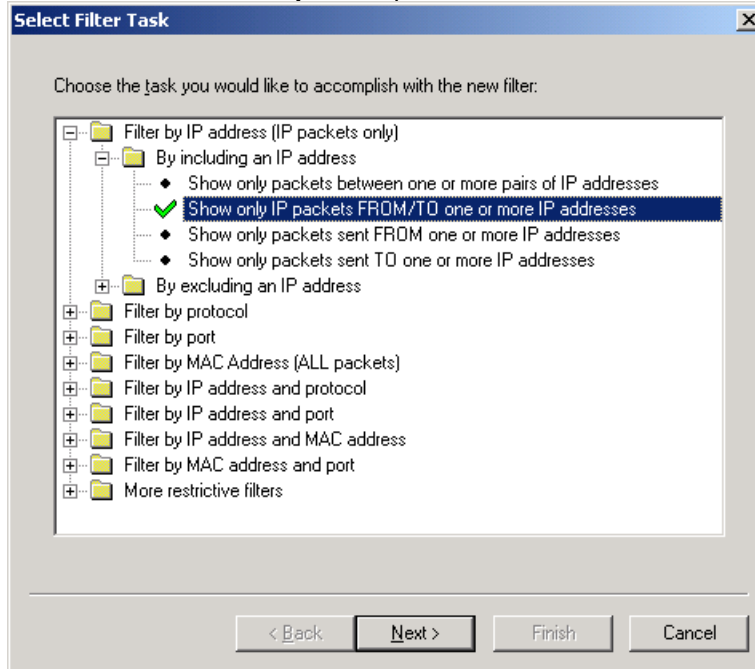


Creating a Filter with the built-in Templates

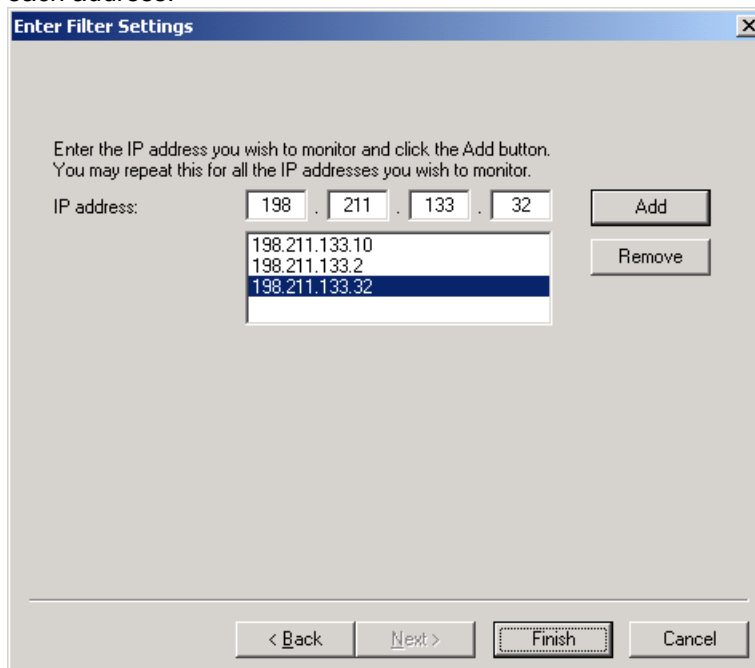
The built in templates allow you to build efficient filters without getting involved with logical expressions. They are very easy to use and cover most basic filtering needs. With these templates you can quickly create filters that will capture the traffic from or to specific IP addresses or systems, that are sent to or from a specific port, that contain a particular protocol such as HTTP or most combinations of these. To build a filter using the built-in templates:

Using Filters

1. Choose the **built-in templates** option, then click the **Create** button.



2. You will see a tree that lists the main filter topics. Open the tree of interest to you. In the example above, we have opened the tree to create a filter that will capture only IP-type packets that are sent from or received by specific IP addresses.
3. When you have selected your template, you will see a green check mark next to the option, click the **Next** button to build the filter.
4. Enter the Filter name as you wish it to appear in the list of filters and a brief description, then click **Next**.
5. Enter the IP addresses whose traffic you wish to monitor one at a time, clicking Add after each address.



6. When you have added all your entries, click Finish. Your filter is now created and will appear in the Existing Filters list. You may now apply this filter to your next captures by setting it as the filter to use in the Capture configuration tab or you can use it on an existing capture file by opening the capture file and then selecting the filter from the filter pull down in the toolbar.

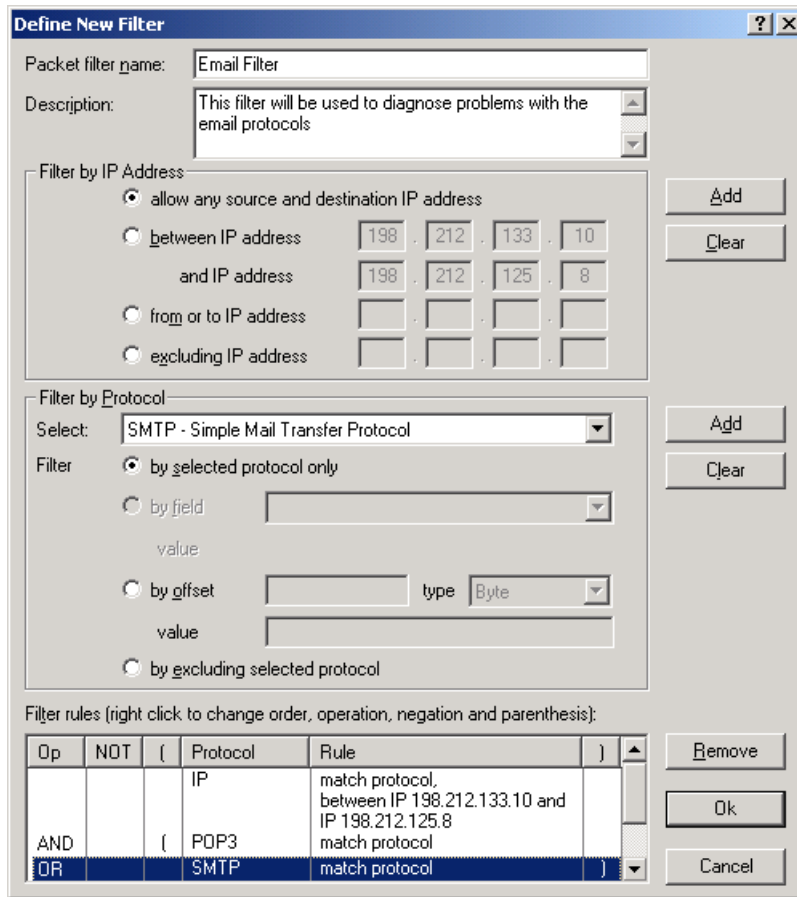
Note: If you wish to set the capture filter, you must do this before starting a capture. A capture filter is applied through the **Settings** command in the **Capture** menu.

Creating a Basic Filter Using Advanced Expressions

To create a new filter:

1. Select **Filters** in the **Configure** menu.
2. Select **Advanced Expressions** and then click on **Create**. Give your filter a descriptive name. For example, if you are going to write a filter for the email protocols you may want to call your filter Email Filter.
3. In the description field write a short description that will later remind you why you created this filter.
4. You may choose to restrict the capture to certain systems that you are having a problem with. For example, if you are trying to diagnose a problem between Jim's system and the email server, check the **Filter by IP address** option, and select the **Between IP address** radio button. Then add the IP addresses of Jim's system and of the mail server and click the **Add** button. This will filter unneeded packets from your capture making it easier to read and faster to diagnose the problem.
5. Next you need to select the protocols to filter. In our example of the email protocols you would probably select POP3, IMAP and SMTP. These need to be added one at a time by selecting the protocol and clicking the **Add** button.

- When you have selected all the protocols and any other restrictions that should be part of the filter click **OK** to create the filter.



Note: If you wish to set the capture filter, you must do this before starting a capture. A capture filter is applied through the **Settings** command in the **Capture** menu.

Creating Advanced Filters with Advanced Expressions

The **Advanced Expressions Option** allows for the creation of highly sophisticated filters. Not only are you able to filter by protocol but by an offset within the protocol having a specific value or by giving a value to predefined fields in the packet such as the source hardware address for ARP packets. If the value is a hexadecimal number you need to precede the number by 0x. For example 000186A0 should be entered as 0x000186A0. It is also possible to build filters using logical AND and logical OR.

When filtering by offset, note that the offset is starting from the particular protocol that is currently chosen. If you wish to have the offset from the start of the packet, then you will need to use Ethernet or Token Ring as the protocol. Note that this may give you unexpected results as the packet may also include optional fields that you were not expecting to be in the packet.

Filters may also be created by excluding certain protocols instead of including them. So for example you could create a filter that includes all RPC packets but excludes UDP, which means that only RPC packets over TCP will be filtered.

Filtering by Offset

You can create very useful filters using the packet offset. Below we give an example of how to create a filter that will show only the RPC Portmapper request packets.

1. Select **Filters** in the **Configure** menu.
2. Select **advanced expressions** and then click on **Create**. Give your filter a descriptive name. For example, Filter Portmapper packets.
3. In the description field write a short description that will later remind you why you created this filter.
4. Next you need to select the protocols to filter. Choose **RPC - ONC**.

Modify Filter

Packet filter name:

Description:

Filter by IP Address:

- between IP address . . .
- and IP address . . .
- from or to IP address . . .
- excluding IP address . . .

Filter by Protocol:

Select:

Filter:

- by selected protocol only
- by field
- by offset type
- value
- by excluding selected protocol

Filter rules (right click to change operation, negation and parenthesis):

Op	!	(Protocol	Rule)
			RPC	double word 0x000186A0 at offset 12	
AND			RPC	double word 2 at offset	

5. Now select the Filter **by offset** radio button. Add the offset 12, which is the offset for program number. Set this to Double word and enter the value 100,000, which is the program number for the portmapper application, in hexadecimal format. Note that the hexadecimal number must be preceded by 0x. Click the **Add** button. Next add the offset 16, which is the offset for the version number. Set this to Double word and enter the value 2, which is the portmapper version. Click the **Add** button.
6. Click **Ok** to create the filter.

Filtering by Field

Some of the protocol filters have predefined fields that you can select to filter. As an example of how to do this we will create a filter that will show only TCP and UDP packets coming in and out of port 443.

1. Select **Filters** in the **Configure** menu.

Using Filters

2. Select **advanced expressions**, and then click on **Create**. Give your filter a descriptive name. For example, Filter for Port 443.
3. In the description field write a short description that will later remind you why you created this filter.
4. Next you need to select the protocol to filter. Select **TCP**.

Modify Filter

Packet filter name: Filter on Port 443

Description: This filter will filter all traffic in and out of port 443 and discard all other packets.

Filter by IP Address

between IP address

and IP address

from or to IP address

excluding IP address

Filter by Protocol

Select: UDP - User Datagram Protocol

Filter

by selected protocol only

by field

Destination port

value: 443

by offset

type: Byte

value:

by excluding selected protocol

Filter rules (right click to change operation, negation and parenthesis):

Op	!	(Protocol	Rule)
			TCP	source port 443	
OR			TCP	destination port 443	
OR			UDP	source port 443	
OR			UDP	destination port 443	

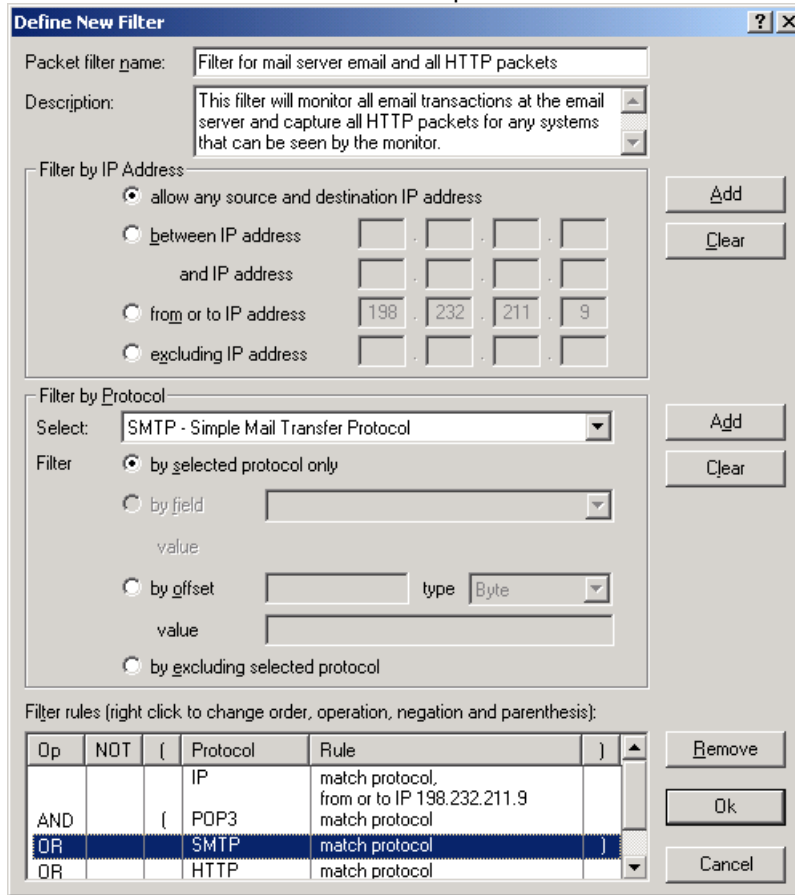
5. Select the Filter **by Field** radio button and choose **Source Port** from the pull down list box. Enter 443 as the value. Click the **Add** button to add this rule to your filter.
6. Now choose **Destination port** from the pull down list box. Enter 443 as the value. Click the **Add** button to add this rule to your filter.
7. Repeat steps 4 to 6 for the **UDP** protocol.
8. Your rules are now complete. Click **Ok** to create this filter.

Building Filters with Mixed Operands

As of version 4, it is possible to build filters with mixed operands. So, for example if you wished to build a filter that filters the SMTP protocol from one system AND all HTTP traffic, this is what you would do:

1. Select **Filters** in the **Configure** menu.
2. Select **advanced expressions**, and then click on **Create**. Give your filter a descriptive name.
3. In the description field write a short description that will later remind you why you created this filter.

- Choose from or to IP address and enter the IP address of the mail server. Now choose SMTP and POP3 and HTTP from the protocol to filter and Add them one at a time.



- Next you need to build the filter statement. Right click the mouse under the column showing an open parenthesis “[” right at the start of the statement and select **Add Open Parenthesis**. Move to the close parenthesis column on the SMTP line, right click the mouse and choose **Add closing parenthesis**. Now move to the last line that contains the HTTP statement, right click on the AND operand, and select **Use OR operation**. The statement is now complete.

Applying a Filter to the Capture

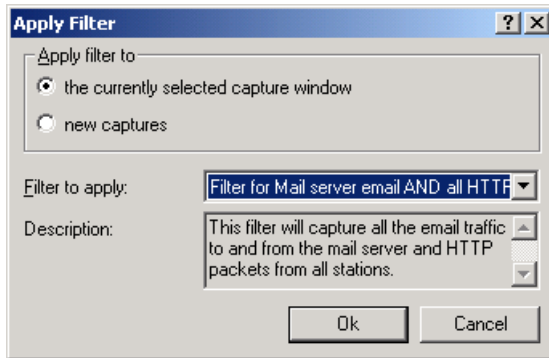
A filter may be applied to the capture itself, thus avoiding the collection of data that is not needed to diagnose your problem. To do this you must set the Capture filter in the **Capture Settings** dialog box in the **Configure** menu. Once the filter is set here, it will remain active for all subsequent captures and must be either removed by choosing <do not apply a filter> or set to a new filter when it is no longer needed. The Capture Filter may also be reset through the **Apply Filter** command in the **Capture** menu.

Applying a Filter to an Existing Capture File

To apply a filter to a network capture that is already completed, you must first load the file into the Network Monitor if it is not already loaded. Then select **Apply Filter** from the **Capture** menu and select **apply filter to the currently selected capture window** and choose the filter to be applied. Click the **OK** button (you may also use the filter combo box in the toolbar to select a filter to apply

Using Filters

to the currently loaded file). The current capture will be immediately filtered using the rules in the specified filter.



Saving the Results of a Filtered File

Once you have applied a filter to a file, you may save the result to a new file by selecting the **Save As** command in the **File** menu.

Releasing a Filter

Once selected a filter will remain active until it is released. If the filter is active only on the currently displayed capture file, then you can release the filter by selecting <do not apply a filter> from the pull down filter box in the toolbar. If on the other hand your filter is active at capture time, then you must release this by selecting <do not apply a filter> in the **Capture Settings** before taking the next capture.

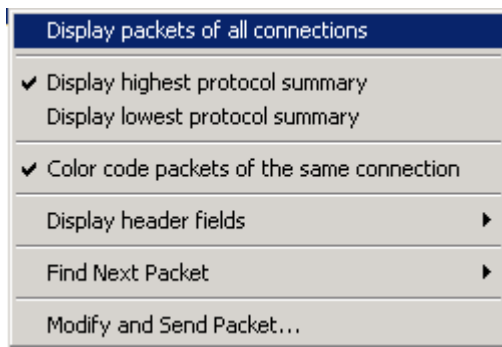
Managing your Filters

Once created, filters may be modified or duplicated by selecting the **Filters** in the **Configure** menu. Just select the filter to be modified, duplicated, renamed or deleted and then click on the appropriate action button.

5 - Viewing your Capture File

Customizing the way you View a Capture File

The Distinct Network Monitor includes a number of features to aid you in viewing the portion of your capture that is most useful to you as efficiently as possible. It includes both general display options that can be set by selecting **Display Settings** in the **Configure** menu as well as very specific display options that become available when you right click the mouse on a specific packet in the one of the Network Monitor windows. In the Summary Window right click the mouse to display the following menu options:



Display only Packets of this Connection

This option is extremely handy and allows you to quickly look through the packets related to a specific TCP connection. Note this feature is only available when you are currently positioned on a TCP packet. For example, as you scroll through your summary window and come across a problem, right click the mouse and select this option. Now you will see only those packets that are part of this TCP connection. The default number of connections whose history is kept is 64, depending on your memory availability, this may be increased as needed in the Advanced Configuration tab. You will need to close the application and start it again when changing this value.

Display Highest Protocol Summary

This is the default display for the Summary window and displays the highest level of protocol in the packet summary line. For example if the packet is an FTP packet it will display this here.

Display Lowest Protocol Summary

This option will display only the lowest level protocol for a packet in the Summary window. For example it will display Ethernet, Token Ring or PPP.

Color Code Packets of the same Connection

This allows you to turn the color-coding of packets of a single connection off. Color-coding is actually very useful as it helps you quickly distinguish the different connections.

Display Header Fields

Display header fields allows you to customize which packet header fields will be displayed in the Summary Window. Changes made to the display fields will be remembered by Network Monitor for subsequent monitoring sessions. The header fields to be displayed may also be selected through the Headers tab in the Configuration menu.

<input checked="" type="checkbox"/> Packet Number
<input checked="" type="checkbox"/> Length
<input type="checkbox"/> Date and Time
<input checked="" type="checkbox"/> Time (in seconds)
<input type="checkbox"/> Delta (in seconds)
<input type="checkbox"/> Source MAC Address
<input type="checkbox"/> Destination MAC Address
<input checked="" type="checkbox"/> Source IP Address
<input checked="" type="checkbox"/> Destination IP Address
<input checked="" type="checkbox"/> Source Port
<input checked="" type="checkbox"/> Destination Port
<input type="checkbox"/> TCP Sequence
<input type="checkbox"/> TCP Acknowledgement
<input type="checkbox"/> TCP Flags
<input type="checkbox"/> TCP Window
<input checked="" type="checkbox"/> Description
Select All
Default Settings

The following are the different packet header fields that can be selected:

Packet Number

This is the sequence number of the packet in the capture. Each packet capture will start from one.

Length

Shows the total packet length.

Date and Time

Displays the actual date and time when the packet was captured.

Time (in seconds)

Gives the lapse in time between the start of the packet capture and time that this packet was received.

Delta (in seconds)

Gives the time in seconds since the previous packet was received. This can come in useful when checking round trip time.

Source MAC Address

Displays the MAC address of the system that is sending the packet. Note that if there is a proxy server on the network this will be the address of that server.

Destination MAC Address

This is the MAC address of the system that received the packet.

Source IP Address

This is the IP address of the system that initiated the packet. Note that if there is a proxy server on the network this will be the address of that server.

Destination IP Address

This is the IP address of the system to which the packet is directed.

Source Port

This is the port from which the packet was sent.

Destination Port

This is the port on which the packet was received.

TCP Sequence

The sequence number is a number that identifies the bytes in the stream of data between the sending and receiving systems. For each new connection the sender allocates an initial sequence number for the connection. Subsequent sequence numbers for packets of the same connection will be incremental.

TCP Acknowledgement

The acknowledgement number is the last sequence number received plus 1. This is valid only if the ACK flag is on.

TCP Flags

The TCP header may have one or more of the following six flags set:

U – this is the urgent pointer flag and is used by protocols such as Telnet and Rlogin to indicate to the client that a portion of the content (data) in this packet should be processed immediately

(possibly ahead of data already in the in buffer for that socket). This is used, for example, to send control characters (such as ^C to interrupt), which should be processed immediately.

A –this is the ACK. It indicates the sequence number of the last data byte, which was successfully received. Every packet except the first in the connection must contain an ACK. If there was no new data, then the previous ACK value is resent.

P – the push flag indicates that the destination should pass this data on to the application as soon as possible. It usually indicates that the packet contains user input and should be processed quickly. However its use is sometimes abused, and some protocols/implementations send everything with push flag.

R – the reset flag is sent whenever a packet segment arrives that does not appear to be correct. It can also be used as a quick way to abort a connection. It tells the other side not to send any more packets on that connection. For example, it is sent if data comes in after a FIN packet.

S – this is the synchronize sequence numbers used to initiate a connection. This is the number of the first byte of data that will be sent over this connection. The other side acknowledges this sequence number by returning it in the ACK field of reply. Both the sequence and the acknowledge numbers are simply the sequence number of a data byte. When sending, the sequence number of the first byte of data in the packet is sent as SEQ, and the sequence number of the last byte received from the other side is sent as ACK.

F – indicates that the sender is finished sending data and that it will close the connection once the other side flushes its outgoing buffer.

TCP Window

This is the TCP windows size. This is the number of bytes available in the in buffer, or, how much data the TCP socket can accept, in addition to the already acknowledged data bytes.

Description

Provides a summarized description of the packet contents. For example it may tell you that the packet is an FTP packet and contains the STOR command.

Find Next Packet

This feature allows you to move from one packet with a protocol error in it to the next without having to scroll through the file. You may either select to go to the next packet with an error or the next packet with an error or warning.

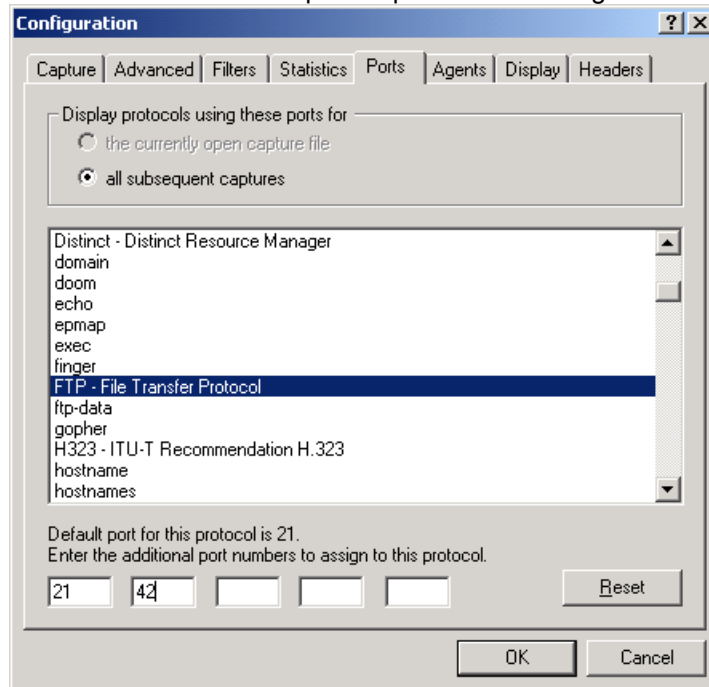
Packets containing a protocol warning are preceded by a white X and packets containing a protocol error are preceded by a black X. You can quickly move from one error to the next in a packet capture file by either selecting the appropriate option from the Capture menu or by pressing CTRL E to move to the next packet that has a protocol error or CTRL W to move to the next packet that has a protocol error or warning.

Modify and Send Packet

This feature allows you to modify and resend a captured packet back onto the network. See the section later in the chapter called Modifying and Resending Captured Packets

Ports and Captured Packets

Distinct Network Monitor parses packets and assigns them to their parsers by PORT number.



By default the Network Monitor will assume that the various protocols are using their default or well-known port. For example, packets communicating on port 23 will be assumed to be Telnet packets. In addition, Network Monitor reads in the port numbers from the Services file on the system it is capturing on and will also use the ports defined there to parse the various protocols. This may, however, not be enough to parse all the packets in a capture taken on a certain subnet. For example, one of the systems in the subnet could be accessing an FTP server connecting on port 42 instead of the normal default port of 21. To parse these packets you need to add 42 as a port for parsing FTP packets. This is done by selecting the **Ports** command in the **Configure** menu and then selecting the protocol for which a port needs to be assigned. In the case of our example this is FTP. Once this is selected you need to add the special port assignment in the next available text box. Click the **OK** button once completed.

When defining additional ports for a specific protocol you may select to use these port definitions only for this capture file or for all subsequent captures.

Searching a Capture File

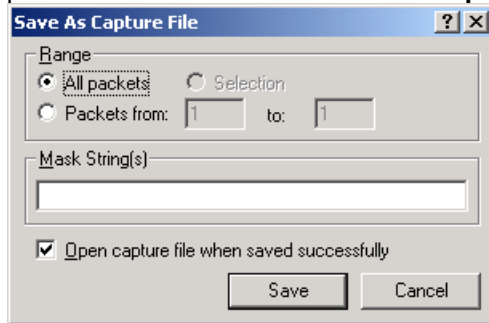
You can easily search for a specific text sting in any packet by using the search capability that is built into the Network Monitor. Either choose the **Search Packet** command from the **Capture** menu or press CTRL+S and enter the string to be searched for in the capture file.

Saving Parts of a Capture File with Another Name

You can save a capture file on which you have applied a filter to another file. This will make it easier for you to navigate through the packets that are of interest to you. You may also save a range of packets from a capture file to another file. For example if you have a large capture file but have identified your problem area to be between packet 5900 and 6100, you could save this

range of packets to a separate capture file. The new file will be much faster to navigate through. To save a filtered file or a packet range from a particular file simply:

1. Select the **Save As** command from the **File** menu.
2. Enter the name of the file it is to be saved as. Make sure that the file type is set to .cap.
3. If you have preselected the packets to save by highlighting them, **Selection** will be automatically selected as the Range. Otherwise select **All packets** or give the range of packets to be saved in the **Save as Capture File** dialog box.

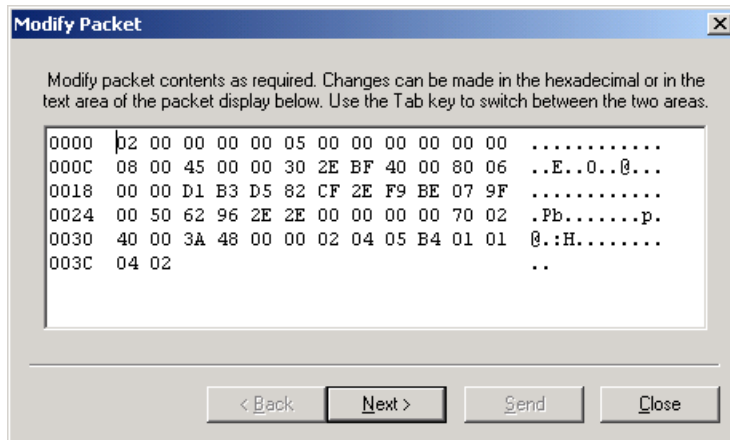


4. Click the **Save** button to actually save the file.

Note: You may also save selected packets from a file that are not necessarily in a sequence. To do this, select all the packets to be saved using the Shift or Ctrl key with the left mouse button, then Select **Save As** from the **File** menu.

Modifying and Resending Captured Packets

Software developers testing their application are able to capture a packet, quickly modify it to test the various needs of their application and resend it on the network. To do this, you need to highlight the packet you wish to test, then right-click the mouse. A hex edit box will be displayed.



You can modify the hex value for the byte you are trying to test by positioning the cursor in front of the character you wish to change and then keying in the new value. When you have finished your modifications, click on the **Next** button.

You can now select the number of times you wish to retransmit the modified packet and the time interval in seconds from one send to the next. If your system has more than one NIC card you must select the card you wish to transmit from, before clicking on the **Send** button.

6- Viewing your Statistics File

The statistics gathered by Distinct Network Monitor can be viewed by clicking on the various topics in the left window of the Statistics.

All IP Traffic

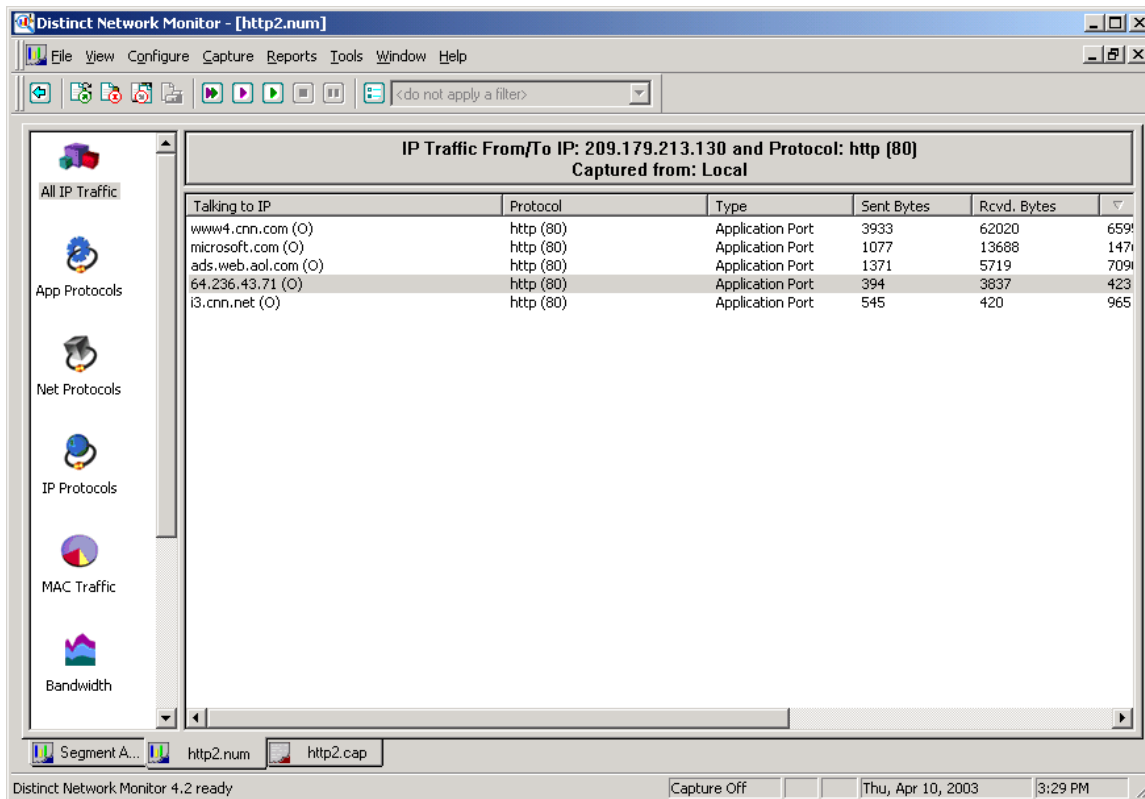
When viewing the All IP Traffic window you will see a graph showing the top 10 talkers in the top window. The bottom window lists all the IP addresses that are active on this network segment. Next to each IP address you will see:

- The IP type – this may be L for local subnet, O for outside of this subnet, B for broadcast and M for multicast.
- The system name
- The number of bytes/packets sent by the system
- The number of bytes/packets received by the system
- The total number of bytes/packets sent and received by the system.

To get more detailed information about the traffic for a particular IP address you need to click on that address. This will show you a detailed breakdown of the different protocols that the particular system has received or sent.

To find out which systems this particular IP address has been communicating with for any of the listed protocols, click on the protocol. This will show you the complete list of IP addresses that the system has been talking to, showing the bytes and packets sent and received.

To go back one level just click on the little blue arrow button in the toolbar or right-click the mouse button to select Go Back.



Whols

We have built in automated Whols queries for you to quickly find out who is the registered owner of any particular IP address or domain name that one of your systems is talking to. To find this out position your mouse on the IP address in question and click on the right mouse button and choose Whols. This will display the registration information for the particular IP and the name of the Whols server that was queried for the information.

Note: If the system listed is not on the same hub, the traffic numbers do not indicate the total traffic for that system, but just the traffic created between it and other systems on the hub or switch being monitored.

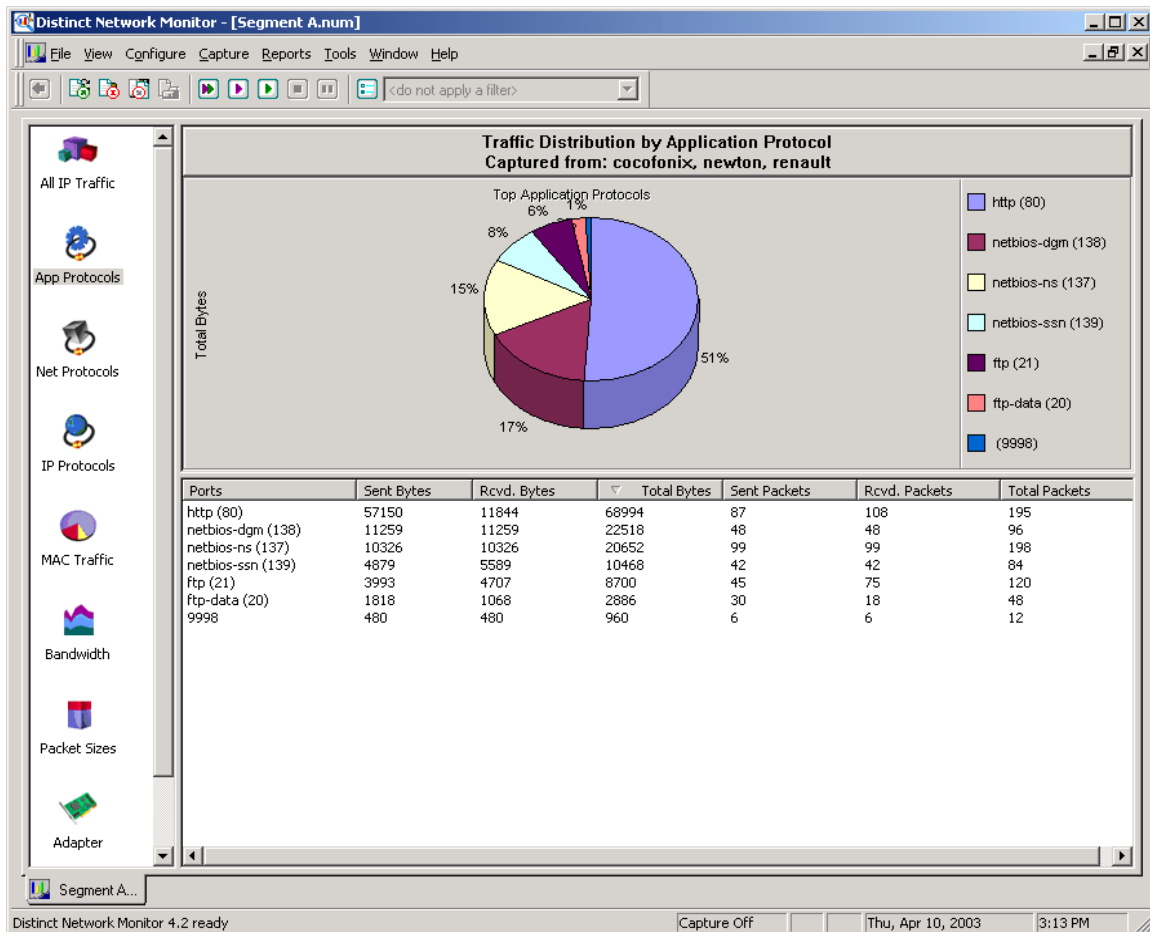
Application Protocols

This displays the traffic distribution by protocol for all traffic that was captured through the specified system.

It shows the list of application protocols showing how many bytes/packets were sent and received for each protocol. Protocols are identified by port number.

To view which IP addresses generated the packets for a particular protocol, click on the protocol name in the first column. This will show the list of IP addresses that generated the traffic and the IP addresses that they were communicating with. To move back one level click on the left arrow button in the toolbar or right-click the mouse button to choose Go Back.

Viewing your Statistics File



Network Protocols

This section shows the list of level three protocols such as IP and Netbeui showing the total number of bytes and packets transmitted for each one. To find out which systems generated the packets for a specific protocol, click on the protocol. This will provide a list of all the local MAC addresses involved in the traffic generation. Note that all packets that are received from outside the subnet will show up as being sent by the router and all packets being sent outside of the subnet will show up as being sent to the router.

IP Protocols

This section lists the IP protocols and the total number of bytes and packets transmitted for each one.

MAC Traffic

This section shows the list of MAC addresses that are active on the local subnet where the monitor is running. For each hardware address the following are displayed:

- IP address

- Bytes Sent
- Bytes Received
- Total Bytes
- Packets Sent
- Packets Received
- Total Packets

This includes all packets whether IP or otherwise that are over Ethernet or Token Ring and may include packets that are not parsed by the Network Monitor.

To get more detailed information on the traffic generated to and from a particular hardware address, click on it. You will see a list of protocols, ports and the number of bytes and packets sent and received. To go back one level click the left arrow.

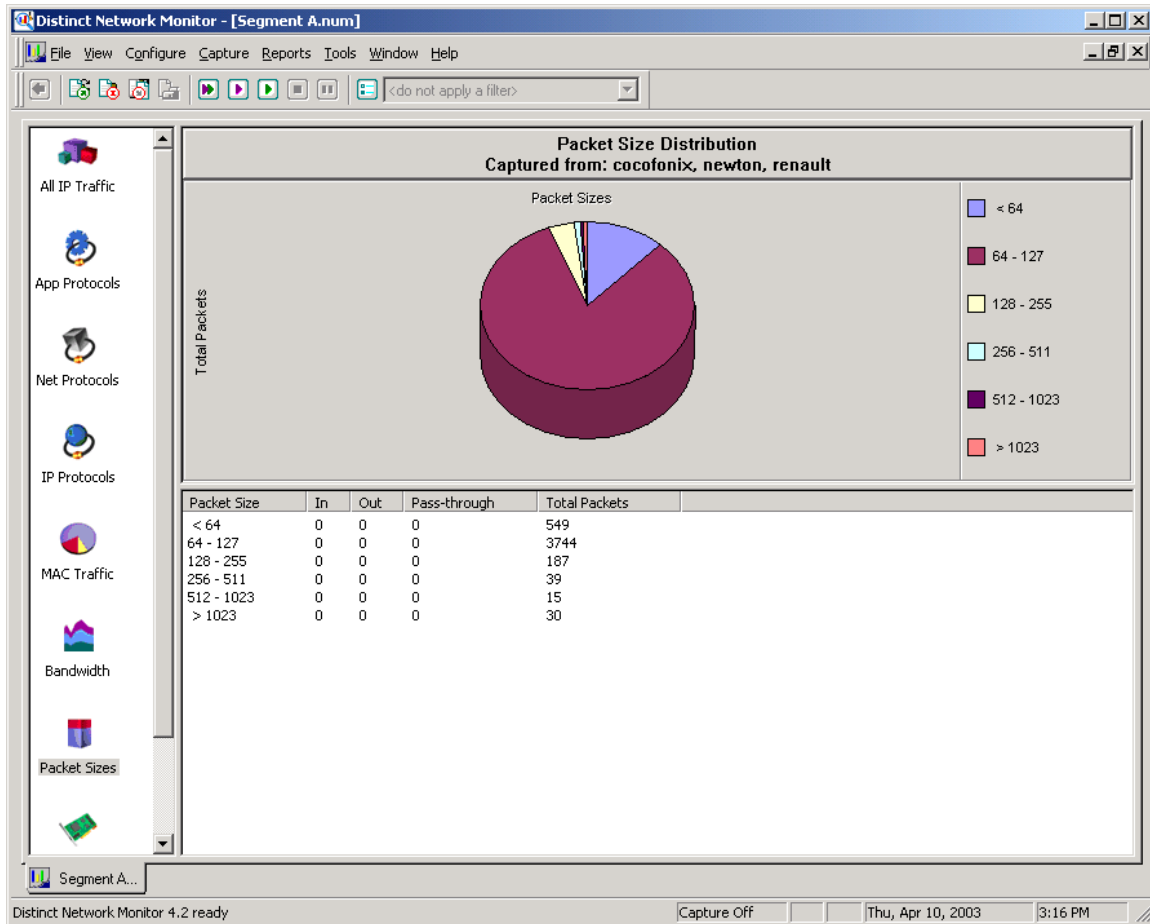
Bandwidth

Bandwidth usage over the specified time period using the number of samples specified. The time and sample size is defined by selecting the **Statistics** option in the **Configure** menu.

Packet Sizes

This section provides an analysis of Packet size distribution showing the number of packets transmitted in various size ranges.

Viewing your Statistics File



Adapter Statistics

This window shows all the statistics that were reported by the NIC driver for the duration of the capture. The statistics displayed depend on the NIC driver. The errors shown here give you an idea on the state of the network segment being monitored.

General Statistics

The following gives an explanation of each statistic in this category. If the NIC driver does not return the statistic, you will see n/a in the list.

Frames not transmitted or transmitted with errors shows the total number of packets transmitted with errors during the time that the network trace was on.

Frames received with errors shows the total number of packets received with errors during the time that the network trace was on.

Frames Missed, No Buffers shows the total number of packets that the NIC cannot receive due to lack of NIC receive buffer space.

Frames received with CRC or FCS errors are the packets received with cyclic redundancy check (CRC) or frame check sequence (FCS) error.

Directed frames/bytes transmitted without errors are the total number of packets that were transmitted directed to a specific IP address

Multicast frames/bytes transmitted without errors are the total number of multicast packets transmitted with no errors. A multicast packet contains a multicast group address in the destination address field of the IP header. Although there may be thousands of intended recipients only one given copy of a packet is generated at source, unlike a unicast packet, which would generate a copy for each recipient.

Broadcast frames/bytes transmitted without errors are the total number of broadcast packets transmitted with no errors.

Directed frames/bytes received without errors are the total number of packets received with the destination IP address in the header.

Multicast frames/bytes received without errors are the total number of multicast packets received with no errors.

Broadcast frames/bytes received without errors are the total number of broadcast packets received with no errors.

Length of transmit queue specifies the number of packets that are currently queued for transmission, on the NIC or in the driver's-internal queue.

Ethernet Statistics

The following describes what each Ethernet statistic reported means. If the NIC driver does not return the statistic, you will see n/a in the list.

Frames received with alignment Errors are the total number of packets received with alignment errors. Alignment errors usually occur when large amounts of data are transferred. Their presence usually indicates an error in the NIC board settings for FIFO threshold.

Frames transmitted with one collision are the total number of packets that are involved in a single collision and subsequently successfully transmitted. Their presence indicates that the network has light to moderate traffic. If this number exceeds 2% of the total transmit packets, this generally means over utilization of the network and is likely to affect the adapter performance.

Frames transmitted with more than one collision are the total number of packets involved in multiple collisions but which are subsequently transmitted successfully

Frames not received due to overrun are the total number of packets that were not transmitted due to an overrun condition. This error may be caused by a receive threshold that is too high.

Frames not transmitted due to underrun are the total number of packets that were not transmitted due to an underrun condition on the NIC.

Frames transmitted with heartbeat failure are the total number of frames successfully transmitted without detection of the collision-detect heartbeat.

Times carrier sense signal loss during transmission are the number of times that the carrier sense signal was lost during transmission.

Late Collisions Detected are the number of collisions detected after the normal window.

Summary

Summary of the statistics recorded during the session and shows whether the Network Monitor driver dropped any packets.

Creating Reports

To create a report of the statistics for a particular capture, select Statistics from the Reports menu and then select the format for your report. You may save the report as an HTML document or in csv format if you intend to import the data into a database.

Reports are saved to the Reports folder under the Network Monitor folder. You may change the folder in which to save your reports by changing the Report Folder path in the Statistics Settings configuration tab.

To generate a report:

1. Make sure that the Statistics file or files for which you wish to generate the report are open.
2. Select **Statistics** from the **Reports** menu, then select the type of report you wish to create, html or csv.
3. The first time you create a report you will get the opportunity to choose your default folder in which to save your reports or accept the one created by the application. All subsequent reports will be created in the same folder. You may change this folder at any time by editing the entry in the Statistics Settings configuration tab.
4. If you currently have more than one report open, you will be asked to select which of the open statistics files you wish to create reports for. Select the files by clicking on them, then click OK to proceed.
5. Now you need to select whether you wish to create your report with all the available statistics or just for select statistics such as the IP statistics only. To deselect an entry just click on it. You can reselect entries by clicking on them again.
6. Click **OK** to generate the report. If you are generating a single report, you will be asked if you wish to open it once it is generated. If you are generating multiple reports, they will be automatically appended to the **Reports** menu. You can open them directly from there. This menu will contain the last 10 reports generated.

7 – Importing and Exporting

The Distinct Network Monitor allows you to import capture files taken with certain other sniffing products and to export a Distinct capture file to a text format.

Converting Third Party Capture Files

Distinct Network Monitor allows you to import a capture file taken by a number of other monitoring products on the market. To do this you must first convert the file into the Distinct capture file format. To do this:

1. Select the **Convert** Command in the **File** menu.
2. Enter the name of the file to be converted and the file name it is to be saved to in the **Convert Capture** dialog box.
3. Click **OK** to start the file conversion. Once the file has been successfully converted, Network Monitor will read it in.

Network Monitor is currently able to import files from the following products:

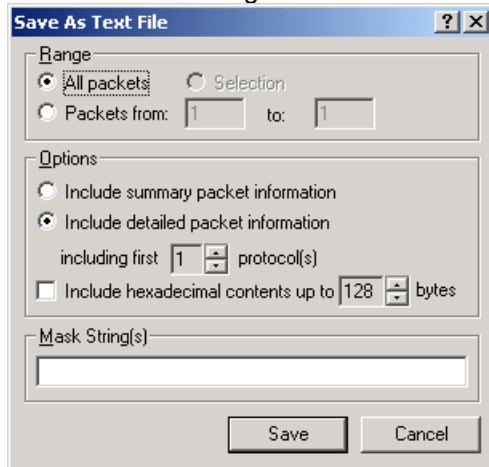
- LanWatch®
- SUN Snoop®
- TCPDump
- Distinct® Network Monitor™ version 2.
- NetXray®
- Novell LANalyzer®

Saving a Packet Capture to a Text File

A Distinct Network Monitor capture file may be saved to a text file. Once in text format, the data may be accessed by any application. To do this:

1. Select **Save As** from the **File** menu.
2. In the **Save As** dialog box, enter the name of the text file you wish to save the packet capture to and make sure that you select Text files as the File Type to be saved.
3. In the **Save As Text File** dialog box, you can select whether to save all the packets or just a range of packets and how much information about the packets you wish to save. You may either select to save just the packet summary or the detailed packet information. If you choose to save the detailed packet information, you must also select how many protocols you wish to save information for. The default value for this is 1. For example, if you select to get details for only one level on HTTP packets, you will only see the details up to the Ethernet level. To see the HTTP details you will need to select 4 protocol levels

instead of one. Doing this will show the details for Ethernet, IP, TCP and HTTP.



4. If you wish to also include the hexadecimal representation of the packets at the end of each packet, then check the **Include hexadecimal contents up to** option. Fill in the maximum bytes you wish to include for each packet.
5. When you have made all your selections, click the **Save** button.

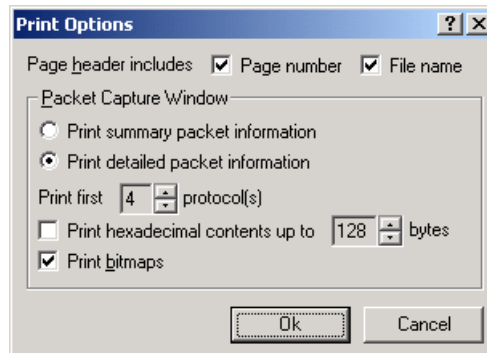
8 – Printing a Capture File

The network packet capture can be printed in whole or in part by using the built-in **Print** command in the **File** menu.

Setting your Print Options

Before selecting the **Print** command be sure to set the print options that you want. To set the print options:

1. Select **Print Options** from the **File** menu.
2. You then need to select whether you wish to print just the packet summary information that is displayed in the top window or the detailed information displayed in the bottom



window. If you choose to print the detailed information you need to also select how many levels of protocols you wish to print out. For example, if you wish to print some IMAP packets and also show the details for TCP, IP and Ethernet, you need to select 4 protocols. The default value for this value is one protocol.

3. You may also choose to print part of the capture in hexadecimal format.

Printing a Capture File

To print the packets you need to select the **Print** command from the **File** menu. This gives you the option to print all the packets in the capture or print only packets within a specified range or to print only the currently selected packets.

9 – Other Tools

The Distinct Network Monitor includes a built-in Ping utility as well as a Traceroute utility program.

Ping

The Ping program is useful to find out whether a system is reachable directly from the computer that is running the Network Monitor. To use simply select **Ping** from the **Tools** menu and enter the name or IP address of the system you are trying to reach.

TraceRoute

TraceRoute allows you to find out the route that a packet will take to get to its destination. Normally TraceRoute uses ICMP packets to do this, you can however select to use UDP packets instead.

Whols

The Whols Utility allows you to find out whom a domain name or IP address is registered to. To make a query:

1. Select the type of query you wish to make. That is by IP address or domain name
2. Enter the IP address or domain name you wish to receive information about in the Domain Name or IP address text box.
3. Enter the Whols server that you wish to query. If you leave this entry on Automatic, we will automatically choose the server that is most likely to be able to resolve the address or domain entered.
4. The results of the query will be displayed in the information area on the dialog box.

Note: If your connection to the Whols server is timing out before you are able to get a response, you may increase the timeout value.

TCP and UDP Connections

This utility shows all the currently open TCP and UDP ports and reports on the status of the TCP ports. Ports may be:

- LISTENING : these ports may either be open ports to which a connection can be made from another system, they can also have a current connection established (in which case you will see the same port number listed as ESTABLISHED or they may be open but in a “hung” position. In this case another computer may not connect to this port. When a port is in LISTENING state and you wish to check whether this is a “hung” connection you can try to scan that same port using the Scan TCP Ports tool.

- TIME-WAIT : This usually means that a port did have an open connection which has been terminated and the port is now about to be closed
- ESTABLISHED : this means that the port is both open and has an active connection going.

Scan TCP Ports

The Scan TCP ports tool allows you to scan one or a range of ports on one or more systems to find out which ports on that system are open and do not have a session currently established. Please note that if you are scanning a large range of ports it will take some time to complete the scan, since the program attempts to connect to each port within the specified timeout value. Other features in the Network Monitor will not be available until the scan is completed.

This tool will report whether it has found a port open or was unable to connect to the port.

You may set the number of times that the application should try to establish a connection with any of the ports it is scanning as well as the time it should wait before it times out waiting to connect.

Note Ports that are currently open and have an established connection will show up as ports for which a connection attempt failed.

Base Conversion

This utility allows you to quickly convert numbers from hexadecimal to decimal or octal and vice versa.