NetDecoder™ Software Analyzer

Ethernet Network View and Ethernet Dashboard

Overview of Features

CONTENTS

INTRODUCTION

This document provides an overview of the Ethernet Network View and Ethernet Dashboard features of the NetDecoder software protocol analyzer.

ETHERNET NETWORK VIEW

The Network View is a graphic depiction of network nodes and connections between them as indicated by packets received by the analyzer. Information shown includes node statistics, node addresses and names, node pair (i.e. conversation) statistics, and network statistics.

Access the Network View either by selecting Network View from one of the View menus on other dialogs or by pressing the Network View icon on one of the other dialogs.

The Network View consists of the following dialogs:

- The main Network View dialog
- A Node Database dialog
- An Edit Alias dialog
- A Set Count For Top N Filter dialog

Network View Visual Elements

The main Network View dialog consists of the following visual elements:

- **The Title Bar**

The Title Bar shows the name of the current capture file (if any).

- **The Menu Bar**

The Menu Bar contains pull-down menus with selections for all functions in Network View.

  - **File** - Allows you to hide/show the Toolbar and Status bar, and also Exit
  - **View** - Allows you to open the Dashboard, Frame Sizes, and Node Database dialogs
  - **Statistics** - Allows you to activate/deactivate various statistics
  - **Addresses** - Allows you to hide/show various address types
  - **Names** - Allows you to hide/show various name types
  - **Format** - Allows you to choose between Exploded, Oval, and Branched layouts. Also allows you to hide/show types of data.
  - **Filter** - Allows you to manage the type and amount of information displayed.
  - **Help** - Opens the Help files

- **The Toolbar**

The Toolbar contains buttons for display selection, and frequently used functions.

- **The Detail Window**

The Detail window displays each node, connections between nodes, various user-selectable statistics and addresses, and mouse hover information windows (aka tooltips). This window has a set of tabs just above it which provide filter selection.

- **The Statistics Graph Window**

The Statistics Graph window displays a subset of the node information that is displayed in the Detail window in list format. This window displays the statistic selected in the Sort by drop-down box located at the top of the window. The Statistics Graph window lists the selected statistic in descending order, along with the topmost Name/Address (as it is displayed in the Detail window).

- **The Overview Window**

The Overview window provides the ability to scroll and zoom the spatially oriented Branched Layout in the Detail window, and display all or part of the network

Note: This window appears only in Branched Layout.

- **The Status Line**

The Status Line appears just below the Detail window, and displays various totals and states.

- **The Instruction Line**

The Instruction line appears just below the status line, and contains some simple instructions for the user.

The Network View dialog is re-sizable and contains a right-click menu. The “Packets” indicator in the lower-right corner is identical to those on the Control Window and Frame Display.

Display Node Information

The user has complete freedom to specify as many or as few statistics, addresses, and names as are desired and in whatever order is desired. There are ten statistics selections and six name/address selections available for display with each node. Selections to display or remove node information can be made using one of the menus at the top of the dialog (Statistics, Addresses, and Names), or by selecting icons in the toolbar. Select Show Lines and Dots Only from the Format or right-click menu to hide all node and conversation information in the Detail window, and select it again to display information.

Node Statistics

To display a node statistic in the Detail window, simply select the statistic from the Statistics menu or select the appropriate icon from the toolbar. The selected statistic appears at the bottom of the upper list associated with each node in the Detail window. When a statistic is selected, its associated icon appears depressed and its menu item is checked. To remove the statistic from the display, simply select it again. To place the statistic at the top of the node list, press and hold the Ctrl key while selecting the statistic.

Select from among the following:

- Bytes Received (BR)
- Bytes Sent (BS)
- Bytes Total (BT)
- Nodes In (NI)
- Nodes Out (NO)
- Nodes Total (NT)
- Packets Received (PR)
- Packets Sent (PS)
- Packets Total (PT)
- Utilization (UT)
- Show All Conversations
- Hide All Conversations
- Show Visible Conversations as Bytes (CB)
- Show Visible Conversations as Packets (CP)
- Hide Zero Count Statistics

Node Addresses

To display a node address in the Detail window, simply select the address from the Address menu or select the appropriate icon from the toolbar. The selected address appears at the bottom of the lower list associated with each node in the Detail window. When an address is selected, its associated icon appears depressed and its menu item is checked. To remove the address from the display, simply select it again. To place the address at the top of the node list, press and hold the Ctrl key while selecting the address.

Select from among the following:

- IP Address (IP)
- MAC Address (MC)
- Named MAC Address (NM)
- Order of Appearance
- Hide Empty Addresses and Names

Node Names

To display a node name in the Detail window, simply select the name from the Names menu or select the appropriate icon from the toolbar. The selected name appears at the bottom of the lower list associated with each node in the Detail window. When a name is selected, its associated icon appears depressed and its menu item is checked. To remove the name from the display, simply select it again. To place the address at the top of the node list, press and hold the Ctrl key while selecting the name.

Select from among the following:

- Alias (AL)
- DNS Name (DN)
- NetBIOS Name (NB)

- Automatically Resolve IP to DNS - You must select this option to use the Show DNS Names on the Dashboard
- Hide Empty Addresses and Names

Node Information Display Options

In addition to the individual selection options described above, you have several other options for displaying information using the Format menu:

- Display all node information by selecting Show All Node Info
- Hide all by selecting Hide All Node Info icon
- Restore Node Info to return the display to its original state

Displaying Conversation Information

Conversation Statistics

Conversation statistics display on the lines between nodes.

1. Select *Show Info for All Conversations* from the *Format* or *right-click menu*, or simply click the toolbar icon.
2. Choose the units to display by selecting *Show Visible Conversation as Bytes* or *Show Visible Conversation as Packets* from the *Statistics* menu.
3. In the event that the Detail window becomes crowded, the conversation statistics may become hidden behind the node statistics display.
4. Select *Put Lines and Conversations On Top* from the Format or right-click menu, or click the icon on the toolbar.
5. Select the menu item again or click the toolbar icon to place the conversation statistics in the background.
6. To hide all conversation statistics, select *Hide Info for All Conversations* from the Format or right-click menu, or simply click on the toolbar icon.

Quick Tip:

To view statistics for a subset of conversations:

- Hover the mouse pointer over the desired node conversation to highlight the line (the line turns magenta to indicate selection)
- Right-click and select *Show this Conversation*.
- Select the menu item again to hide the conversation statistics.

Adding/Editing an Alias for a Node

Specifying aliases

An alias is an arbitrary string up to 200 characters in length that the user can define and associate with any MAC address. Each MAC address can have a different alias. Aliases are remembered between sessions and apply to all live captures and capture files. Each alias takes effect as soon as the OK button is pressed on the Edit Alias dialog.

Add/Edit an Alias

1. Click the *Node Database* icon or select *Node Database* from the *View menu* on the Network View dialog to open the Node Database dialog.
2. Select the row containing the alias you want to add/edit
3. Click the *Edit Alias* button (or simply double click the row) to open the Edit Alias dialog. (Note that during live capture, entries in the Node Database may be moving around, which can make it difficult to select the entry you want.
4. Add/edit the alias in the text box and click OK.
5. Repeat steps 2 and 3 until all aliases you want to change are completed
6. Close the Node Database dialog.

Quick Tip:

If you need to only add/edit one alias, then hover the mouse pointer over the desired node in the Detail window, right click, and select *Edit Alias* from the menu to open the Edit Alias dialog.

Filter and Sort the Network View

Filtering

The *Filter* menu and the tabs above the detail window set the current filter. The filter is always applied to the current sort. Changing the sort criterion may change which nodes are filtered in and which are filtered out.

- **Unfiltered**: Shows all nodes
- **No Broadcasts**: Hides the broadcast node and its conversation lines (i.e. the orange dot and all orange lines disappear).
- **Top N [Sort by selection]**: This shows the top N nodes or conversations based on the statistic listed on the tab (the current sort). The “N” value defaults to 10, but can be set to any value.
- **Top N [Sort by selection], No Broadcasts**: Hides the broadcast node and its conversation lines, then displays the top N of the remaining nodes or conversations based on the statistic listed on the tab (the current sort). The value of N is the same value used in the Top N filter.
- **Always Shown**: This shows all nodes that have been marked via the right-click menu as being always shown. The right-click menu makes it possible to specify that the current node, the current node pair (if the mouse cursor is on a conversation line), or all currently selected nodes always be shown (those selected nodes retain this attribute even after they’re unselected). The *Undo “Always Shown” for All Nodes* icon in the toolbar, along with selections in the right-click and Format menus, removes this attribute from all nodes. Marking a node as always shown not only ensures that it is always visible regardless of which filter is in effect (inclusion mode), but also makes it possible to isolate nodes by clicking on the Always Shown tab (isolation mode). When a node is visible solely because it’s always shown, a little white dot is drawn in the center of it. Thus an always shown node is always visible when the top N filter is in effect, but only when it is not in the top N does it contain a white inner dot. In this way a node’s statistics and whether it is in the top N can be monitored simultaneously.

Sorting

In the Network View, one sort or another is always in effect. Select the statistic to sort on from the Sort by drop-down box above the Statistics Graph. The sort in effect is displayed on the Top N tabs and in the Statistics Graph in descending order. The sort order determines which nodes appear in the Detail window when one of the Top N filters is applied.

Setting the Count For Top N Filters

The Set Count for Top N Filters is an option on the Network View.

1. Click the *Set Count For Top N Filter* icon, or select Set Count For Top N Filter from the Format menu to display the Set Count For Top N Filter dialog.
2. Enter a new value for N and click OK.

The new value of N appears on the Top N filter tabs on the Detail window.

Detail Window Layouts

There are three layout possibilities for the Detail window, each of which provides a different degree of flexibility. Layouts are selected from the Format menu or by selecting icons on the toolbar. Select Use Black Background from the Format or right-click menu to display a black background in the Detail window.

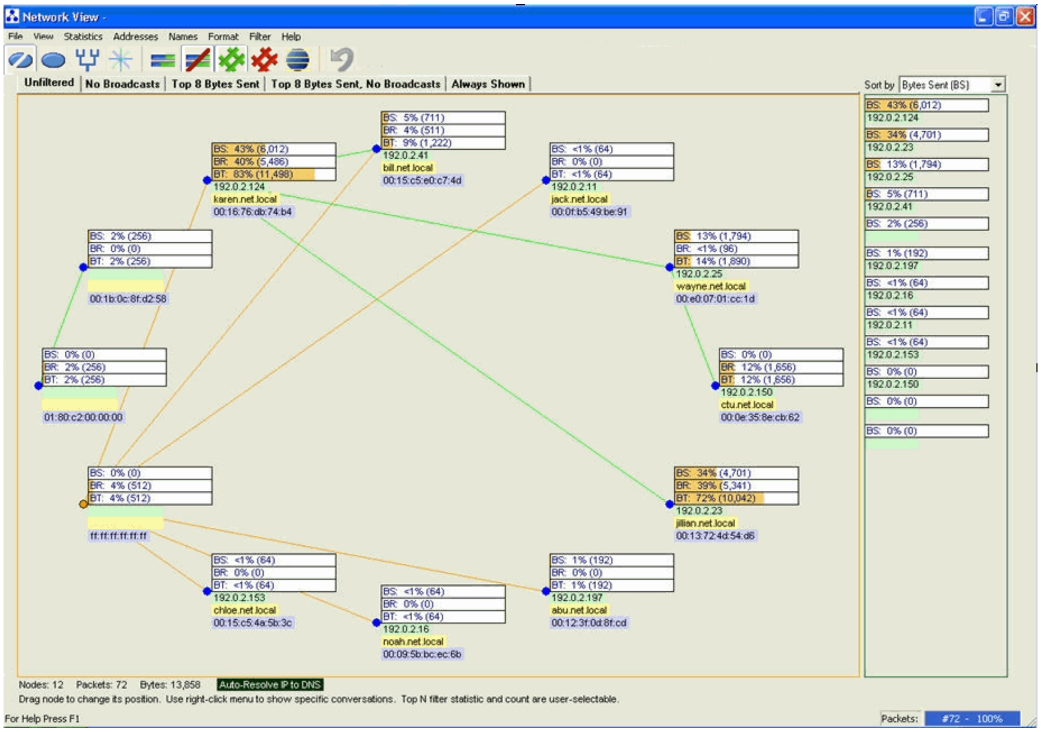
Exploded Oval Layout

Exploded Oval Layout shows nodes evenly arranged in an oval shape in the Detail window. Click the *Exploded Oval Layout* icon or select *Exploded Oval Layout* from the Format menu to display this layout.

Oval Layout

Oval Layout also shows nodes in an oval, but instead of arranging them evenly around the oval it leaves gaps where nodes have been filtered out. Since nodes don't move (except for the slight rotation around the oval that occurs each time a new node is discovered and added), this makes it easy to see nodes appear and disappear as they are filtered in and out. On the other hand, it can be more congested than Exploded Oval Layout and thus harder to read. Click the *Oval Layout* icon or select *Oval Layout* from the Format menu to display this layout.

Both Exploded Oval Layout and Oval Layout leave gaps for nodes that the user has dragged (see Positioning Nodes in the Detail Window below). In both of those layouts, the oldest node is at the far right and halfway up the detail window (i.e. at the 3 o'clock position). The next oldest node is just above it, and the newest node is just below it. When a node appears for the first time, it is placed just below the oldest node, and the other nodes rotate clockwise around the oval.

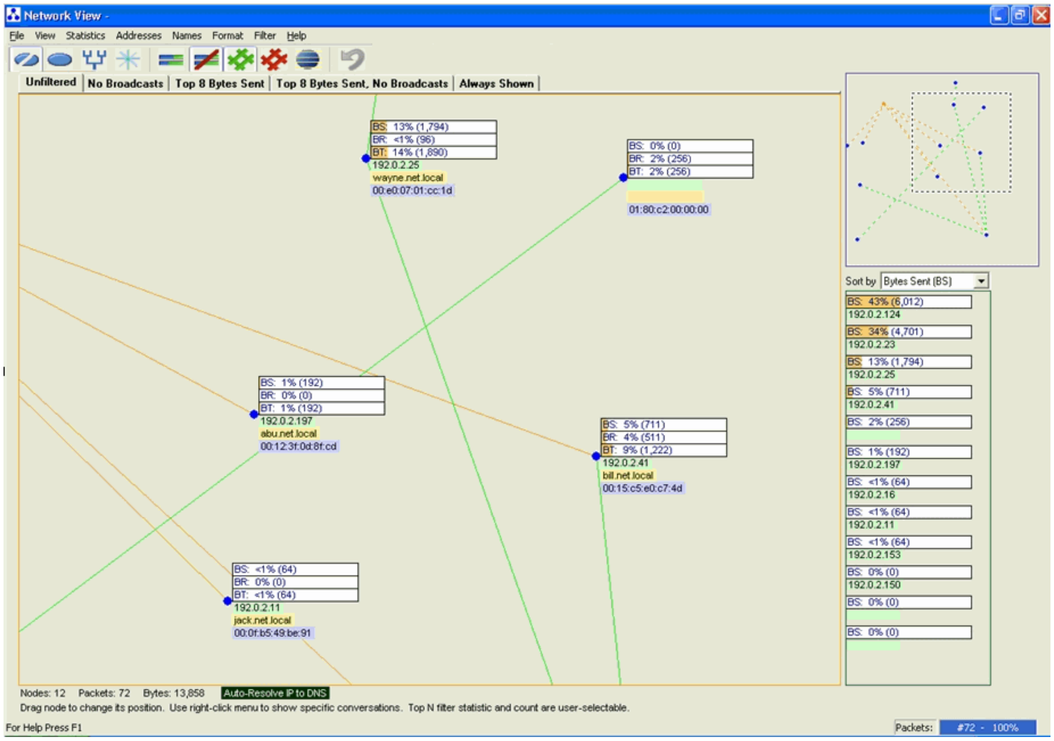


Drag node to change its position. Use right-click menu to show specific conversations. Top N filter statistic and count are user-selectable.

Figure 1: Network View Oval Layout

Branched Layout

Branched Layout shows nodes in a free format, and also shows an Overview window which contains a zoomable and movable viewport that can be used to focus the Detail window on a specific area of the network. Branched Layout assigns node positions randomly. Click the *Branched Layout* icon or select *Branched Layout* from the Format menu to display this layout



Nodes: 12 Packets: 72 Bytes: 13,858

Drag node to change its position. Use right-click menu to show specific conversations. Top N filter statistic and count are user-selectable.

For Help Press F1

Figure 2: Network View - Branch Layout

Positioning Nodes in the Detail Window

- Oval Layouts

Nodes can be selected and dragged in either Oval layout. A dragged node is not auto-located in either of the Oval layouts, so it provides a means in those layouts for a user to freeze the position of a node. Nodes can be dragged singly or in groups. Select multiple nodes either by using Ctrl-click or by enclosing desired nodes in a box created by dragging the mouse. Simply click in any vacant area of the Detail window to de-select. Dragged nodes can be moved back into the oval of the current Oval layout by clicking the *Move Dragged Nodes Back Into Oval* icon or by selecting *Move Dragged Nodes Back Into Oval* from the Format menu.

- Branched Layout

Nodes can be selected and dragged in the Branched layout. Nodes can be dragged singly or in groups. Select multiple nodes either by using Ctrl-click or by enclosing desired nodes in a box created by dragging the mouse. Simply click in any vacant area of the Detail window to de-select. To see any nodes that have been dragged outside of the Detail window, select *Reformat Branched Layout* from the Format menu to re-position all nodes within the window.

The Statistics Graph Window

The Statistics Graph window displays, in list format, a subset of the node or conversation information displayed in the Detail window. This window is always sorted in descending order of the statistic displayed. The statistic that appears in this window can be one of ten Node statistics, or one of two Conversation statistics, and is user controlled.

- **Node Statistics**

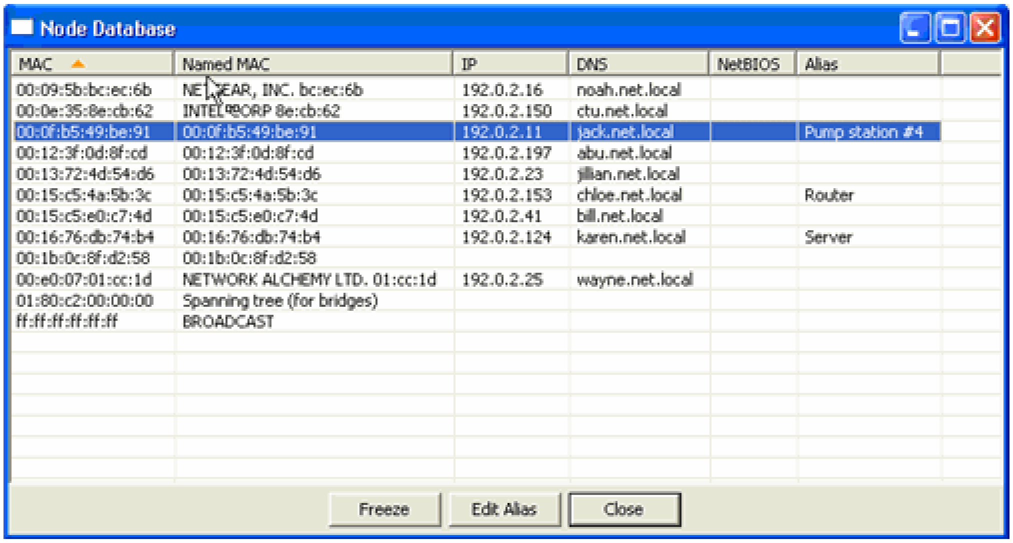
When a node statistic is chosen as the sort criterion, the Statistics Graph displays the selected statistic and the topmost address/name (as it appear in the Detail window) for each node displayed in the Detail window. The statistic line for each node displays the abbreviation of the selected statistic, its percent value, and its actual value. The only exception is Utilization, where only the actual value is displayed. The statistics line also functions as a bar graph that displays the percent value of the statistic from left to right. This list sorts in descending order and has scroll capability.

- **Conversation Statistics**

When either Conversation Bytes (CB) or Conversation Packets (CP) statistic is chosen as the sort criterion, the Statistics Graph displays the selected conversation statistic, and the topmost addresses/names (as they appear in the Detail window) for the corresponding pair of nodes displayed in the Detail window. The statistic line for each node displays the abbreviation of the selected conversation statistic (CB or CP), its percent value, and its actual value. The statistics line also functions as a bar graph that displays the percent value of the statistic from left to right. This list sorts in descending order and has scroll capability.

The Network View Node Database

The Node Database dialog shows node addresses and names in a sortable table. It is kept up-to-date with the Network View main dialog at all times unless the Freeze button on the Node Database dialog has been pressed, in which case no new rows are added (individual fields within each entry are still updated however). The purpose of the Freeze button is to keep the table entries in one place while the user is in the process of adding aliases. The display can be sorted on any column in ascending or descending order simply by clicking on the column header. The sort in effect, and the direction of the sort, is indicated by a pointer in the column header. The sorted column is sorted such that blank entries always appear at the bottom of the column.



Node Database

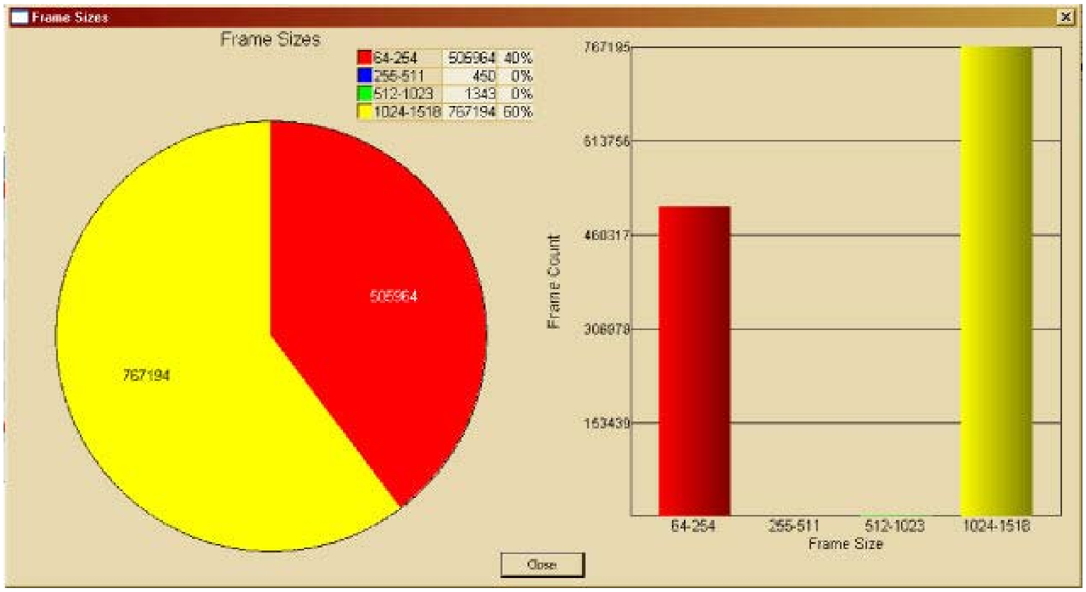
MAC ▲	Named MAC	IP	DNS	NetBIOS	Alias
00:09:5b:bc:ec:6b	NETGEAR, INC. bc:ec:6b	192.0.2.16	noah.net.local		
00:0e:35:8e:cb:62	INTEL CORP 8e:cb:62	192.0.2.150	ctu.net.local		
00:0f:b5:49:be:91	00:0f:b5:49:be:91	192.0.2.11	jack.net.local		Pump station #4
00:12:3f:0d:8f:cd	00:12:3f:0d:8f:cd	192.0.2.197	abu.net.local		
00:13:72:4d:54:d6	00:13:72:4d:54:d6	192.0.2.23	jillian.net.local		
00:15:c5:4a:5b:3c	00:15:c5:4a:5b:3c	192.0.2.153	chloe.net.local		Router
00:15:c5:e0:c7:4d	00:15:c5:e0:c7:4d	192.0.2.41	bill.net.local		
00:16:76:db:74:b4	00:16:76:db:74:b4	192.0.2.124	karen.net.local		Server
00:1b:0c:8f:d2:58	00:1b:0c:8f:d2:58				
00:e0:07:01:cc:1d	NETWORK ALCHEMY LTD. 01:cc:1d	192.0.2.25	wayne.net.local		
01:80:c2:00:00:00	Spanning tree (for bridges)				
ff:ff:ff:ff:ff:ff	BROADCAST				

Figure 3: Node Database

Frame Sizes

The Frame Sizes window is accessed from the *Network View* > *View menu*.

The window displays the percentage of captured data in four byte size ranges: 64-0254, 255-511, 512-1023, and 1024-1518 in a pie chart and a vertical graph.



🟥 64-254	505964	40%
🟦 255-511	450	0%
🟩 512-1023	1343	0%
🟨 1024-1518	767194	60%

Figure 4: Frame Sizes

Resolving DNS Names in Network View

IP addresses are resolved to DNS names in two ways: automatically or manually. Resolution is achieved via network query, and is the only instance in which the Network View places a message on the network. In auto-mode, at most one resolution is attempted per second to ensure that Network View-generated traffic is minimal. Other processing continues while this resolution is underway.

- **Resolve DNS Names Automatically for All IP Addresses**

Select *Automatically Resolve IP To DNS* from the Names menu or from the right-click menu.

A check mark appears next to the menu item and the text *Auto-Resolve IP to DNS* appears in the Status line just below the Detail window.

To stop auto-resolve, simply select (un-check) the menu item again.

- **Resolve DNS Names Manually for Individual IP Addresses**

If you need only resolve one or two IP addresses, then hover the mouse cursor over the desired node in the Detail window and select *Resolve IP to DNS* from the right-click menu. Once resolution is complete, the DNS for the selected node appears in the node's list (ensure that DNS Name is selected as a list item).

Network View Technical Notes

Information Gathering and Processing

- Packets are used to obtain addresses and compute statistics for each node, each pair of connected nodes, and for the network as a whole.
- System query is used to resolve IP addresses to DNS names.
- Aliases are specified by the user.
- Node statistics are saved for each occurrence of each MAC address in each packet. A complete list of node and conversation statistics is given in a table below.
- Conversation statistics are saved for each pair of MAC addresses from each packet, and is direction-specific.
- Network statistics are simply a total of all of the node statistics.
- Since statistics are saved by MAC address, a changing IP address does not change the computed statistics.

Information Storage

The obtained and computed information is saved when a live capture is saved to a capture file. When the capture file is reopened, the stored information is retrieved and used without having to reprocess the packets in the capture file.

Textual and Graphical Representation

Each node is represented as a dot, and one or more conversations between a pair of nodes are indicated by a single line connecting the two corresponding dots. Dots are normally blue and lines are normally green, but broadcasts are shown as orange lines that are connected to a single orange dot that does not represent an actual node and whose sole purpose is to provide a broadcast endpoint.

Node statistics, addresses, and names are displayed to the right of each node in the Detail window. Statistics are displayed above the centerline of the dot that represents the node. Addresses and names are displayed below the centerline.

With the exception of utilization, each statistic is displayed as a little horizontal single-item bar graph which shows the count and percentage as text and uses the bar to graphically represent the percentage. A text prefix and text color-coding indicate which statistic it is (see table below).

Utilization does not show a percentage. Instead, it uses color-coding to indicate its absolute value (see table below).

Addresses and names have color-coded backgrounds: MAC = purple, Named MAC = cyan, IP = light green, DNS = yellow, NetBIOS = blue, and Alias = light red.

There can be any number of statistics, addresses, and names displayed for each node, and these are selected via the icons in the toolbar at the top of the main Network View dialog. The order of display follows the order of selection from top to bottom, except that selecting an icon via a Ctrl-click puts that item at the top of the list instead of at the bottom.

Node or conversation data is displayed in the Statistics Graph depending on the selection made in the Sort by combo box above the graph. The entries in the Statistics Graph are sorted by descending statistic value.

Conversation data is displayed along each line that connects two nodes and is direction-specific. Either byte count or packet count can be displayed (this is done via the Format menu, right-click menu, or by selecting the Conversation Bytes or Conversation Packets icons in the toolbar). These statistics are displayed as single-item bar graphs which always hug the line connecting the nodes, rotating as the line is rotated. The statistic text flips as the user moves the line through vertical so that the text is never upside-down. A little arrow at the end of the statistics box indicates the direction of the conversation. The colors in a conversation statistic bar graph (green on blue) are different from the colors in a node statistic bar graph (orange on white) so that it's easy to distinguish between them.

User Defined Settings

User defined settings and display options listed below persist across sessions.

- Layout selection
- Positions of dragged nodes in Oval Layout and Exploded Oval Layout
- Positions of all nodes in Branched Layout
- Filter selection
- Count for Top N Filter setting
- Sort order selection
- Always Shown node selections
- Node statistics, addresses, and names selected for display
- Conversations displayed and statistic selected
- Put Lines and Conversations On Top selection
- Detail window background color selection
- Show Lines And Dots Only selection
- Auto-resolve IP addresses to DNS names selection
- Aliases

Node and Conversation Statistics:

Prefix	Type	Bar Graph?	Text Color	Bar Graph Color	Description
BR	Node	Yes	Blue	Orange on White	Bytes Received
BS	Node	Yes	Blue	Orange on White	Bytes Sent

BT*	Node	Yes	Blue	Orange on White	Bytes Total (Bytes Received + Bytes Sent)
NI	Node	Yes	Green	Orange on White	Nodes In
NO	Node	Yes	Green	Orange on White	Nodes Out
NT**	Node	Yes	Green	Orange on White	Nodes Total
PR	Node	Yes	Red	Orange on White	Packets Received
PS	Node	Yes	Red	Orange on White	Packets Sent
PT*	Node	Yes	Red	Orange on White	Packets Total (Packets Received + Packets Sent)
UT	Node	No	See following table	See following table	Utilization (Megabits/Sec over the last 10 seconds, counting both Bytes Sent and Bytes Received)
CB	Conversation	Yes	Blue	Green on Blue	Conversation Bytes
CP	Conversation	Yes	Red	Green on Blue	Conversation Packets

**The Bytes Total and Packets Total statistics each add up to 200% since they count each byte twice, once at the sending node and once at the receiving node.*

*** The Nodes Total statistic counts unique nodes, so it's not simply a sum of nodes sent to and nodes received from. For example if node A sends to only nodes B and C and receives from only node B, its total node count is 2, not 3.*

Here is utilization coloring:

Utilization (Megabits/Second)	**Colors**
<0.01	Black on White
>= 0.01 and < 2	White on Dark Blue
>= 2 and < 3	Black on Yellow
>= 3	White on Dark Red

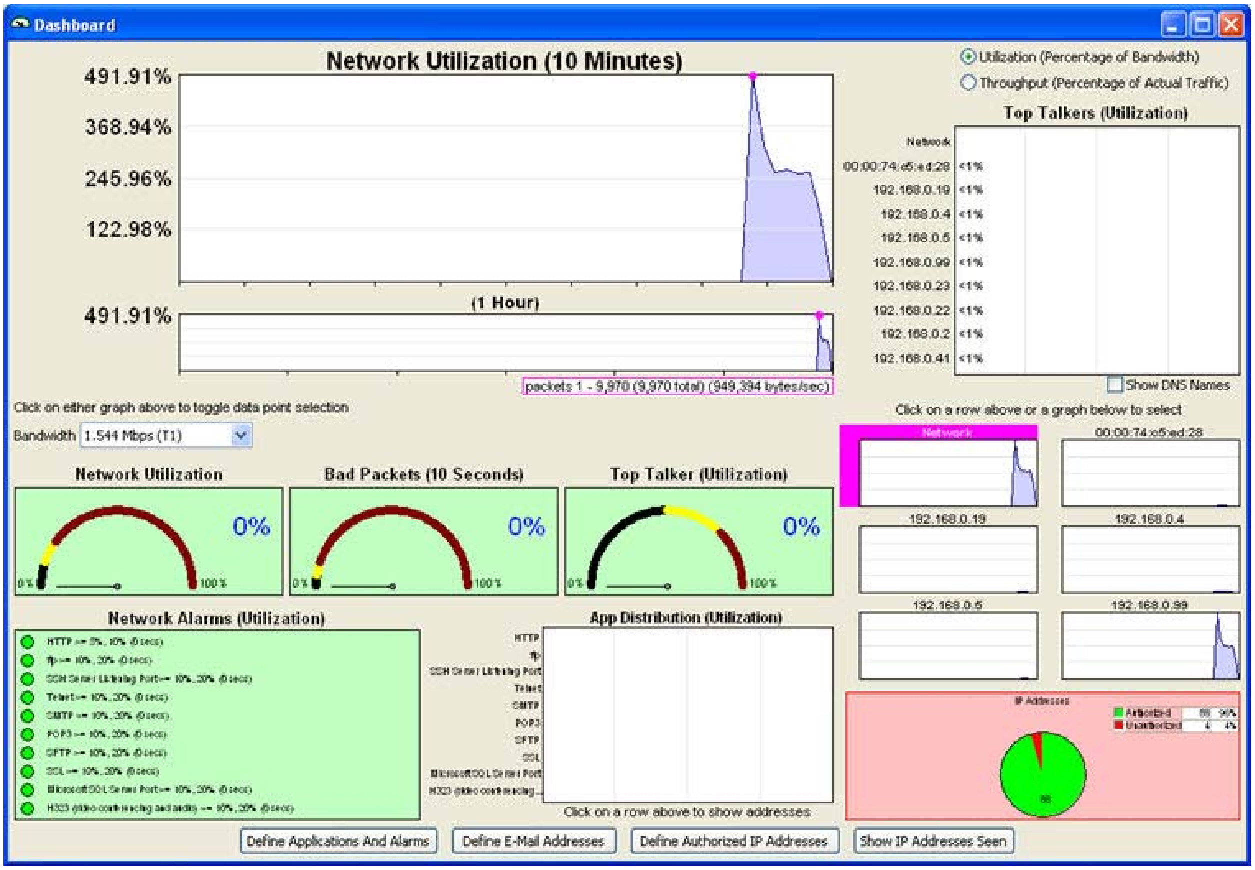
Utilization for each node is shown as megabits/second and is computed over the last 10 seconds, even if the node has been present for less time than that. Both bytes sent and bytes received are counted, so if there are only two devices A and B on the network and all that is happening is that device A is sending to device B, both of those devices display the same utilization.

A mouse hover information window (aka tooltip) showing all statistics, addresses, and names can be displayed for each node. The tooltip background is normally yellow, but since the nodes can move, the tooltip background turns green and the text "*** Node not under mouse pointer" appears at the bottom of the tooltip when the node moves out from under the mouse pointer or disappears altogether. The tooltip itself, however, persists until the user moves the mouse pointer or presses Esc. The tooltip regains its original yellow appearance if the node moves back under the mouse pointer.

ETHERNET DASHBOARD

The Dashboard View displays a dynamic view of what is occurring on your Ethernet communications network.

You access the Dashboard by selecting *Dashboard* from the View Menu on the Control Toolbar and Network View windows or from the Dashboard icon on the Control Window and Frame Display toolbars.



● Utilization (Percentage of Bandwidth)
○ Throughput (Percentage of Actual Traffic)

packets 1 - 9,970 (9,970 total) (949,394 bytes/sec)

Click on either graph above to toggle data point selection

Bandwidth 1.544 Mbps (T1)

Network	
00:00:74:c5:ed:28	<1%
192.168.0.19	<1%
192.168.0.4	<1%
192.168.0.5	<1%
192.168.0.99	<1%
192.168.0.23	<1%
192.168.0.22	<1%
192.168.0.2	<1%
192.168.0.41	<1%

- HTTP -- 5%, 10% (0 secs)
- ftp -- 10%, 20% (0 secs)
- SSH Server Listening Port -- 10%, 20% (0 secs)
- Telnet -- 10%, 20% (0 secs)
- SMTP -- 10%, 20% (0 secs)
- POP3 -- 10%, 20% (0 secs)
- SFTP -- 10%, 20% (0 secs)
- SSL -- 10%, 20% (0 secs)
- MicrosoftSQL Server Port -- 10%, 20% (0 secs)
- H323 (video conferencing and audio) -- 10%, 20% (0 secs)

Click on a row above to show addresses

🟩 Authorized	88	96%
🟥 Unauthorized	4	4%

Figure 5: Ethernet Dashboard

One Hour/Ten Minute Utilization Graphs

These graphs display network or device utilization (% bandwidth). The top graph displays utilization for the last ten minutes. The graph beneath it displays utilization for the last hour. Select the network or a device by clicking on the Top Talkers chart or on one of the small utilization graphs below it.

A black dot indicates the current data point in both graphs as selected by the position of the mouse pointer. Clicking in either graph turns the dot magenta and freezes its location. Clicking again without moving the mouse pointer horizontally restores the black dot.

Utilization and Throughput

Utilization is measured as a percentage of full channel bandwidth. Throughput is measured as a percentage of the actual traffic.

On the Dashboard, selecting the *Utilization (Percentage of Bandwidth)* radio button affects several areas of the Dashboard:

- **Top Talkers (Utilization) Graph** - Displays utilization (% bandwidth). Shows for network and each device in descending order. Max 10 entries.
- **Bad Packets (10 Seconds) Meter** - Displays % bad packets over last 10 seconds.
- **Top Talker (Utilization) Meter** - Displays utilization (% bandwidth) for device with highest utilization.
- **App Distribution (Utilization)** - Displays utilization (% bandwidth) per specified app for last 10 seconds or since app was defined, whichever is less. Shows the apps in definition order.

Selecting *Throughput (Percentage of Actual Traffic)* radio button affects several areas of the Dashboard:

- **Top Talkers (Throughput) Graph** - Displays percentage of actual traffic sent since the beginning of the session. Shows for each device in descending order. Max 10 entries.
- **Bad Packets Meter** - Displays %bad packets since beginning of session.
- **Top Talker (Throughput) Meter** - Displays percentage of actual traffic sent since the beginning of the session for the device with the highest such percentage.
- **App Distribution (Throughput)** - Displays percentage of actual traffic sent by each app since the app was defined. Shows the apps in definition order.

Top Talkers (Utilization)

This chart displays bytes sent since beginning of session of each device in descending order with a maximum of 10 entries when the Throughput (Percentage of Actual Traffic) radio button is selected.

The chart displays utilization expressed as % bandwidth with a maximum of 10 entries when the Utilization (Percentage of Bandwidth) radio button is selected.

Bandwidth Drop-down

Utilization is % bandwidth. With the Bandwidth drop-down box you can specify that the bandwidth is one of the following (Gbps = Gigabits per second; Mbps = Megabits per second):

1. 1 Gbps
2. 155 Mbps (OC3)
3. 100 Mbps
4. 43.232 Mbps (T3)
5. 10 Mbps
6. 1.544 Mbps (T1)

Network Utilization Meter

The Network Utilization Meter displays the total utilization of all devices on the network. Utilization is % of bandwidth.

Bad Packets Meter

The Bad Packets meter shows % bad packets over the last 10 seconds when the Utilization (Percentage of Bandwidth) radio button is selected.

The Bad Packets meter shows % bad packets since the beginning of the session when the Throughput (Percentage of Actual Traffic) radio button is selected.

Top Talker (Utilization) Meter

The Top Talkers chart displays utilization (% bandwidth) for the network and up to 9 devices when the Utilization (Percentage of Bandwidth) radio button is selected.

The Top Talkers chart displays throughput (percentage of actual traffic sent since the beginning of the session) for up to 10 devices when the Throughput (Percentage of Actual Traffic) radio button is selected.

Data is shown in descending order of value.

Network Alarms (Utilization)

This chart displays the network alarms specified in the Applications and Alarms dialog. For each alarm:

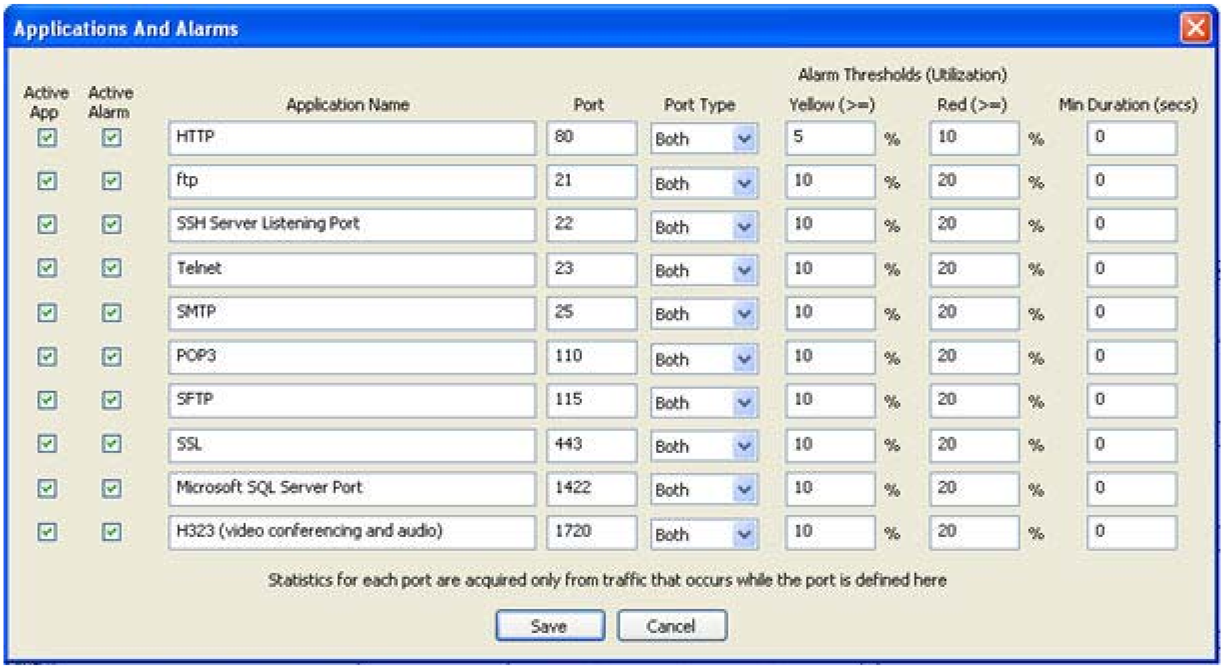
- If the data does not exceed the Yellow threshold level, the table displays green.
- If the data equals or exceeds the Yellow threshold level, the Network Alarms (Utilization) table displays yellow and an e-mail is sent to each e-mail address specified in the E-Mail Addresses dialog.
- If the data equals or exceeds the Red threshold level, the Network Alarms (Utilization) table displays red and an e-mail is sent to each e-mail address specified in the E-Mail Addresses dialog.

IP Addresses

The IP Addresses pie chart displays the number of authorized IP Addresses in green and the number of unauthorized IP Addresses in red

Define Applications and Alarms

The Applications And Alarms window is used to specify which apps are displayed in the App Distribution (Utilization) graph and the Network Alarms (Utilization) table.



Applications And Alarms

Active App	Active Alarm	Application Name	Port	Port Type	Alarm Thresholds (Utilization)				Min Duration (secs)
					Yellow (>=)		Red (>=)		
☑	☑	HTTP	80	Both	5	%	10	%	0
☑	☑	ftp	21	Both	10	%	20	%	0
☑	☑	SSH Server Listening Port	22	Both	10	%	20	%	0
☑	☑	Telnet	23	Both	10	%	20	%	0
☑	☑	SMTP	25	Both	10	%	20	%	0
☑	☑	POP3	110	Both	10	%	20	%	0
☑	☑	SFTP	115	Both	10	%	20	%	0
☑	☑	SSL	443	Both	10	%	20	%	0
☑	☑	Microsoft SQL Server Port	1422	Both	10	%	20	%	0
☑	☑	H323 (video conferencing and audio)	1720	Both	10	%	20	%	0

Statistics for each port are acquired only from traffic that occurs while the port is defined here

Figure 6: Define Applications and Alarms

1. On the Dashboard select the *Define Applications And Alarms* button.
2. Select *Active App* if you want the app to appear in the App Distribution graph.
3. Select *Active Alarm* if you want the app to appear in the Network Alarms (Utilization) table.
4. Enter a name for the app in the Application Name text box.
5. Enter the port number in the Port text box.
6. Select TCP, UDP, or Both from the combo box for the Port Type.
7. Enter a utilization (% bandwidth) value for the low (Yellow) threshold for the Alarm Thresholds (Utilization).

   If the data equals or exceeds the Yellow threshold level, the Network Alarms (Utilization) table displays yellow and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog. For example, if you set a Yellow threshold of 10% for HTTP and the activity equals or exceeds 10% for the specified minimum duration (see below), the background and circle next to HTTP turns yellow and e-mail is sent indicating a Yellow alarm condition.
8. Enter a utilization (% bandwidth) value for the high (Red) threshold for the Alarm Threshold (Utilization).

   If the data equals or exceeds the Red threshold level, the Network Alarms (Utilization) table displays red and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog. For example if you set a red threshold of 15% for HTTP and the activity equals or exceeds 15% for the specified minimum duration (see below), the background and the circle next to HTTP turns red and e-mail is sent indicating a Red alarm condition.

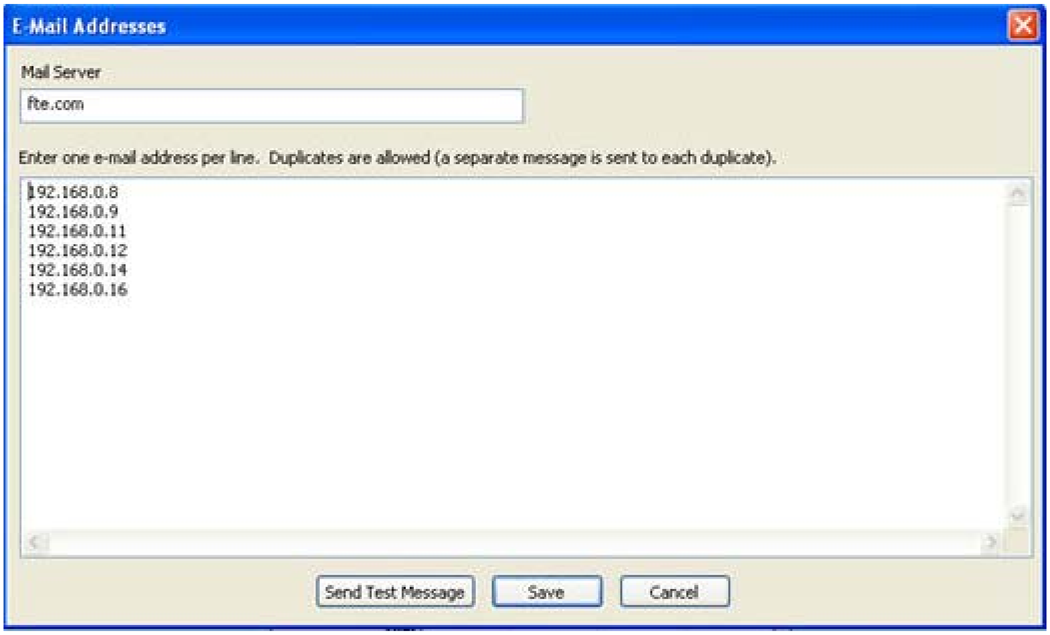
When the alarm clears (i.e. the data returns to a Green condition from either a Yellow or Red condition), the background and the appropriate circle turn green and e-mail is sent indicating that the alarm has cleared.

9. Enter a value (in seconds) for a minimum duration.
   This value identifies how long an alarm threshold must be equaled or exceeded before the alarm is indicated in the Network Alarms (Utilization) table and e-mail is sent. For example, let's say HTTP has a Yellow Alarm Threshold of 10%, with a Min Duration (secs) of 5. This means that the Alarm Threshold of 10% must be equaled or exceeded for at least five seconds for the alarm to show as yellow on the Network Alarms (Utilization) table and for e-mail to be sent. If the value is 0 seconds the alarm is indicated immediately.
10. Select Save

If there are any errors in the settings a message is displayed listing each error. If there are no errors, the settings are saved.

Define Email Addresses

The E-mail Addresses window is used to specify the email addresses that receive a message when an alarm condition is met or when an unauthorized IP address is detected.



E-Mail Addresses

Mail Server

fte.com

Enter one e-mail address per line. Duplicates are allowed (a separate message is sent to each duplicate).

```
192.168.0.8
192.168.0.9
192.168.0.11
192.168.0.12
192.168.0.14
192.168.0.16
```

Figure 7: Define Email Addresses

There are two pieces of information you have to enter: mail server and email addresses.

Mail Server

1. On the Dashboard select Define E-Mail Addresses.

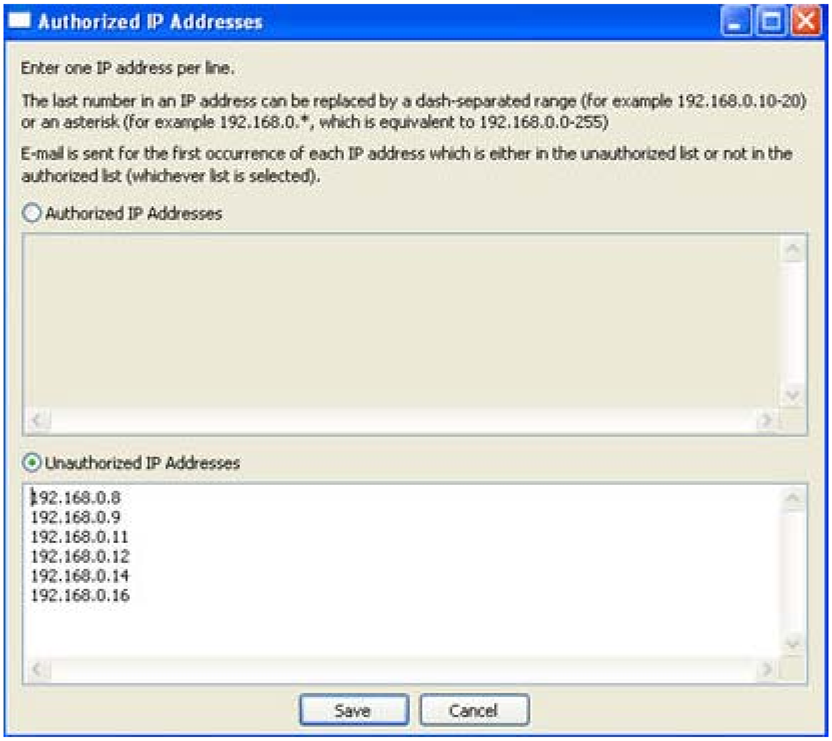
2. Enter the Mail Server address. To locate the Mail Server address in Outlook: *'Tools → Options → Mail Setup → E-mail Accounts → Data Files → Click on Mailbox - [Name] → Settings → General.'* The Microsoft Exchange server: field contains the Mail Server address.

Email Addresses

1. Enter one or more email addresses. Note: You can enter only one email address per line. For multiple addresses, press the Enter key to move to a new line.
2. Select Send Test Message to send a test message to the email addresses.
3. Once you verify that the mail server and email addresses have been entered correctly, Select Save

Define Authorized IP Addresses

The Authorized IP Addresses window is used to specify which packet IP addresses are considered to be authorized and which are considered to be unauthorized.



Authorized IP Addresses

Enter one IP address per line.

The last number in an IP address can be replaced by a dash-separated range (for example 192.168.0.10-20) or an asterisk (for example 192.168.0.*, which is equivalent to 192.168.0.0-255)

E-mail is sent for the first occurrence of each IP address which is either in the unauthorized list or not in the authorized list (whichever list is selected).

○ Authorized IP Addresses

● Unauthorized IP Addresses

```
192.168.0.8
192.168.0.9
192.168.0.11
192.168.0.12
192.168.0.14
192.168.0.16
```

Figure 8: Define Authorized IP Addresses

Authorized IP addresses are specified in the top section. If this section is selected, all other IP addresses are considered unauthorized.

Alternatively, unauthorized IP addresses can be specified in the bottom section. If this section is selected, only these IP addresses are considered unauthorized, and all other IP addresses are considered authorized.

If an unauthorized IP address is detected, an e-mail warning is generated.

By default, all IP addresses are considered authorized.

Counts of authorized and unauthorized IP addresses are indicated in the IP Addresses pie chart. The actual addresses are listed in the Show IP Addresses Seen dialog.

To enter an authorized IP address:

- Select the Authorized IP Addresses radio button.
- Enter an IP address by typing it in or by cutting and pasting from the Show IP Addresses Seen dialog.
- Select Save

To enter an unauthorized IP address:

- Select the Unauthorized IP Addresses radio button.
- Enter an IP address by typing it in or by cutting and pasting from the Show IP Addresses Seen dialog.
- Select Save.

There are several items to remember when entering authorized or unauthorized IP addresses.

- You can enter only one IP address per line.
- The last number in an IP address can be replaced by a dash-separated range (for example 192.168.0.10-20) or an asterisk (for example 192.169.0.*, which is equivalent to 192.169.0.0-255)
- E-mail is sent for the first occurrence of each IP address, which is either in the unauthorized list (if the Unauthorized IP Addresses section is selected) or not in the authorized list (if the Authorized IP Addresses section is selected).

Show IP Addresses Seen

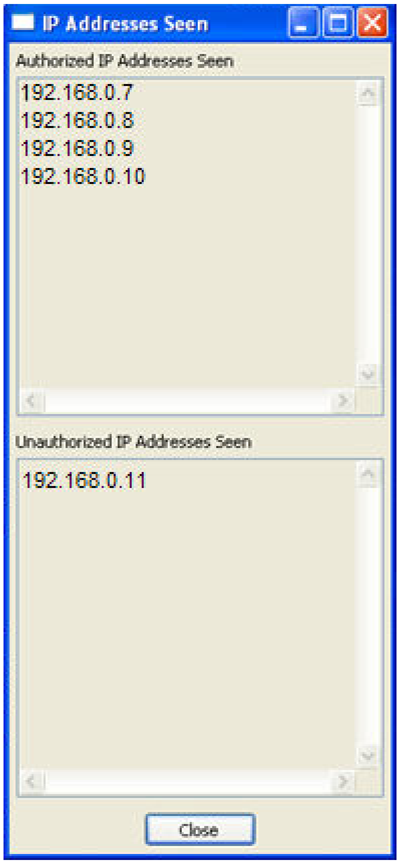
The IP Addresses Seen window displays which IP addresses (source and/or destination) have been detected in packets.

Authorized IP addresses are shown in the top section.

Unauthorized IP addresses are shown in the bottom section.

You specify whether an IP address is authorized or unauthorized using the Authorized IP Addresses dialog.

IP addresses can be selected and copied from both the authorized and unauthorized sections of the dialog and pasted into the Authorized IP Addresses dialog.



IP Addresses Seen

Authorized IP Addresses Seen

192.168.0.7
192.168.0.8
192.168.0.9
192.168.0.10

Unauthorized IP Addresses Seen

192.168.0.11

Figure 9: Show IP Addresses Seen

TECHNICAL SUPPORT

Technical support is available in several ways. Frontline’s website has documentation on common problems, as well as software upgrades and utilities to use with our products.

Web: http://www.fte.com, click **Support**

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505