

LABORATORY WORK NO. 9

PROTOCOL INSPECTOR II – USING CAPTURE FILTERS

1. Objectives

The aim of this laboratory is advanced use of Fluke Networks Protocol Inspector. It will be shown the mode of building filters for different protocols and addresses (detailed explanation of building and modifying a capture filter).

2. Theoretical considerations

2.1 Introduction

Fluke Networks' OPV-PE is an application that runs under Windows (2k, NT 4.x, XP). It's an application for analyzing and monitoring Ethernet 10/100/1000 Networks.

OPV-PE provides users with the most robust, easy to use set of network analysis and monitoring tools in a single package. OPV-PE's user interface provides both a comprehensive view of the network as well as the ability to easily drill down to a specific network segment. OPV-PE's main window provides a single, user-defined view for each of the segments being monitored.

OPV-PE typically interfaces with one or more of Fluke Networks' hardware analyzer tools. OPV-PE can simultaneously capture, monitor, and analyze multiple devices, plus analyze captured data. OPV-PE monitors local network segments; the optional Remote software allows Fluke Networks software to communicate with Fluke Networks hardware and access Fluke Networks products on remote segments.

This lab is based on the lab regarding to Protocol Inspector use, from Local Area Computer Networks class.

2.2. About filters

Using Protocol Inspector you can capture packets, by building filters. Filter Captures are used to get those packets that verify a rule, (i.e. source address or destination address). All in all, you can view packets that come from one or more stations, or packets that leave a station, or both variants. Using Protocol Inspector it's possible to monitor all traffic from a local network, specifying MAC or IP address.

This lab builds examples for capturing packets sent and received by a computer that has Protocol Inspector installed.

2.3 Defining a filter

You can define a simple filter using a single filter template. There are two types of filter templates:

- **Pre-defined Filter Templates:** a pre-defined filter template looks for a specific data pattern or a collection of data patterns. The filter template is supplied by OPV-PE and cannot be changed.
- **Custom Filter Templates:** a custom filter template also looks for a specific data pattern or a collection of data patterns. You can base a custom filter template on a pre-defined filter template or directly enter all data patterns. The most common custom template uses a pre-defined template and adds a conversation or port number. You can also directly enter values at packet offsets in hexadecimal, decimal, or ASCII. Once you have created and saved a custom template, you can always access it from the Available Filter Templates box.

A conversation is a data pattern specific to the source and destination addresses, including the protocol type and the direction of traffic. The Add Conversation to Filter Template area in the display provides a convenient means of adding addresses to a custom filter template.

A port is a data pattern specific to the source and destination port numbers, including the protocol type and the direction of traffic. The Add Port to Filter Template area in the display provides a convenient means of adding port numbers to a custom filter template.

2.4 Using Protocol Inspector to define capture filters

Step1. Open Protocol Inspector (Start->Programs->Fluke Networks-> Optiview Protocol Expert EDV-> Optiview Protocol Expert EDV)

Step2. Double click on the Monitor View or choose Module -> Detail View (F9) from the menu.

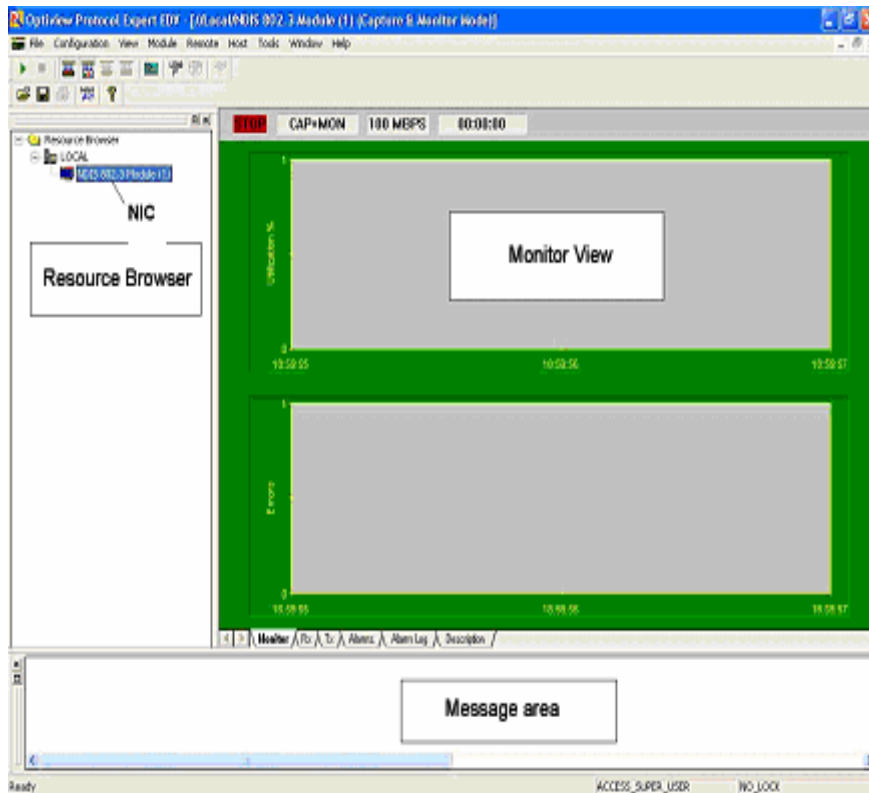


Figure 9.1

Step3. Select Module -> Capture Filter -> Create / Modify Capture Filter from the menu.



Step4. Open the window for selecting the conditions for filtering.

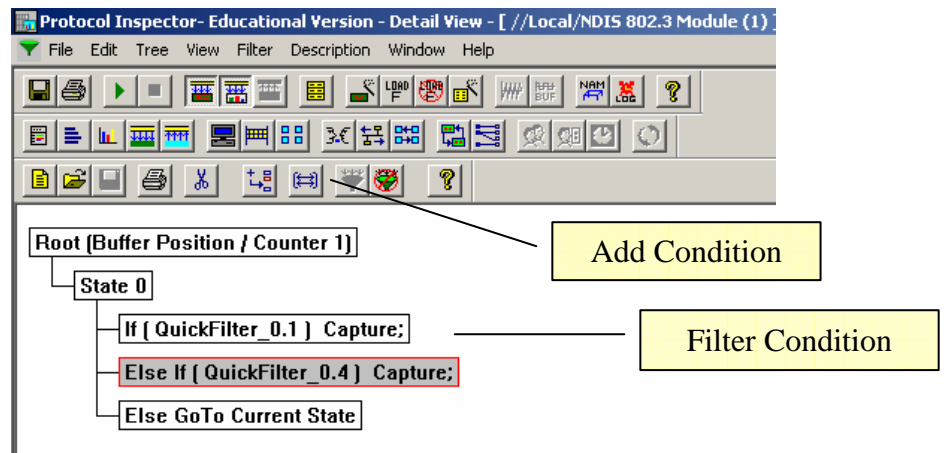


Figure 9.2

Step5. Add the filtering conditions by pressing Add Condition button. Double click on the condition, for editing it, resulting condition edit window. The next example shows how to build the condition to filter all the packages received by KANT.

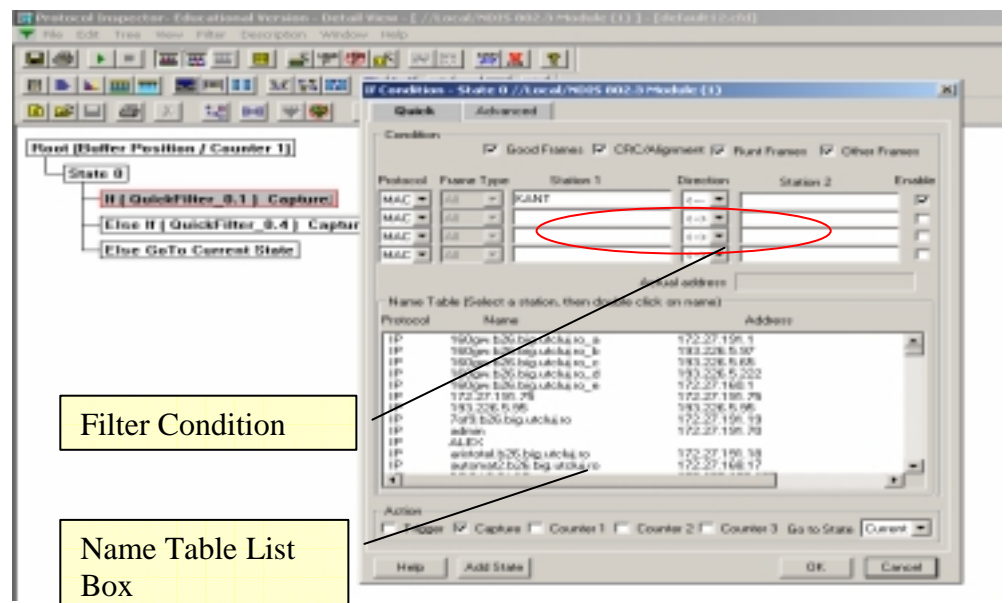


Figure 9.3

PROTOCOL INSPECTOR – USING CAPTURE FILERS

Building a filter means to specify the IP or MAC for the computers you want to monitor, and the direction of transmitting the packages. The direction can be one way or two ways represented by arrows (<-, ->, <->). To accept the conditions built, press OK button.

For Protocol Inspector 5.0.2 the filter window is shown in the next picture.

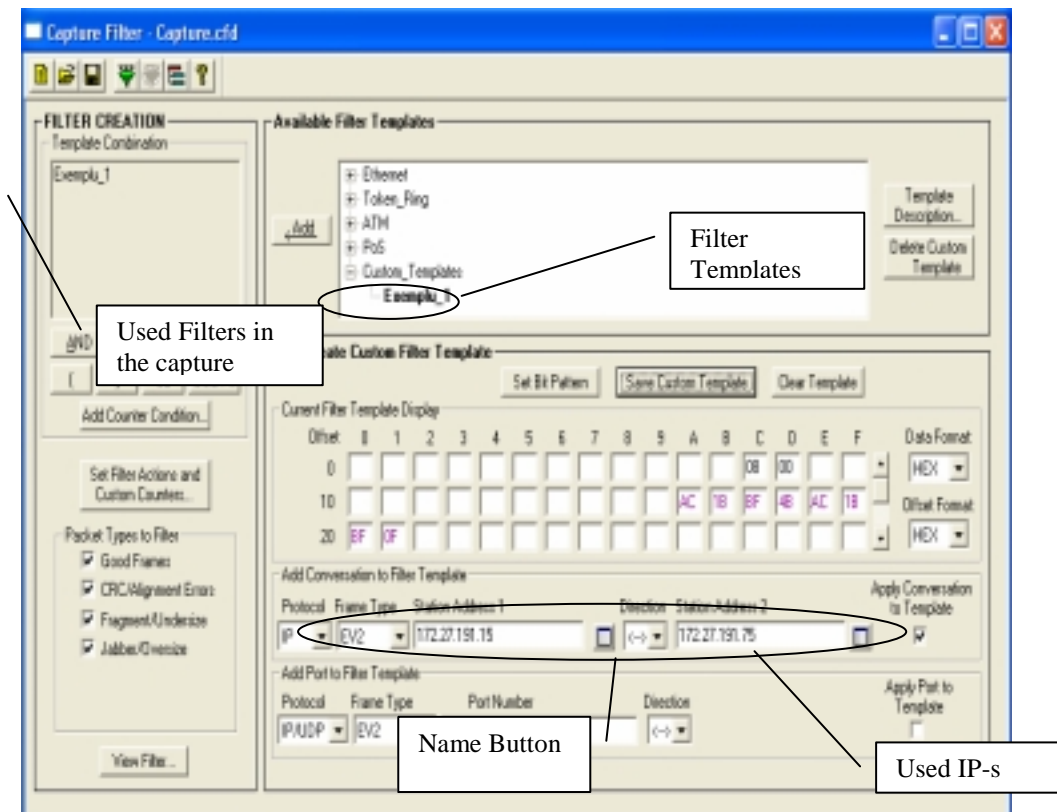


Figure 9.4

A conversation provides a convenient way to add addresses to a filter. You specify conversations for the filter by filling out the Add Conversation to Template portion of the Filter Design window. This portion consists of a protocol selection, frame type selection, two station addresses, a direction indicator, and an enable/disable check box.

Table 9.1 *Defining Conversations*

Protocol	MAC, IP, IPX, or Atalk (AppleTalk)
Frame Type	All, EV2 (EthernetII), SNAP, 8022 (IEEE 802.2), 8023 (IEEE 802.3), ISL, VLAN. Frame type applies to IP-layer addresses only
Station Address 1	Complete IP, IPX, MAC, or ATalk station address
Traffic Direction Indicator	<-> Capture/Display all traffic between Station 1 and Station 2
	-> Capture/Display only the traffic where Station1 is the Source Address and Station 2 is the Destination Address
	<- Capture/Display only the traffic where Station 2 is the Source Address and Station 1 is the Destination Address
Station Address 2	Complete IP, IPX, MAC, or ATalk station address

Apply Conversation to Template check box Enable (include) or disable the conversation as part of the filter template.

The protocol and the frame type are selected from pull-down boxes. OPV-PE automatically restricts you from entering combinations that make no sense.


OPV-PE will automatically set up the correct protocol and frame type when you select a station address from the name table.

Station addresses can be entered directly in the Station Address field or by selecting an address from the name table. Clicking on the Name button brings up the current name table to select an address. The Name Table window shows all name and address associations, including the protocol and the frame type. The name and address associations displayed are those in the currently active name table. Double-clicking on a name table entry will load that name into the currently-selected Station Address field.

If no value is entered for a Station Address field, all stations are captured. For example, if you set an address for Station 1, no address for Station 2, and set the direction to -> all packets having Station 1 as the Source Address are captured, regardless of the Destination Address.

Use wildcards when specifying addresses to capture data on more than one station. An X used as a character for an address string means that any value will be accepted for that position; for example, 343F4AXXXXXX.

To apply the conversation to your filter template, make sure that the Apply Conversation to Template check box is selected. A single conversation is defined. If you want to use additional conversations, you can create an advanced filter or use wildcard characters as described above. After creating the Template, it must be added in Template Combination list box, by pressing Add button (you can create advanced filters).

Step6. In order to activate the filter, it must be loaded, by pressing the Load Filter button, located in the Toolbar menu ().

Note: It's recommended to save the filter before loading it. Press Save button from Toolbar Menu ()

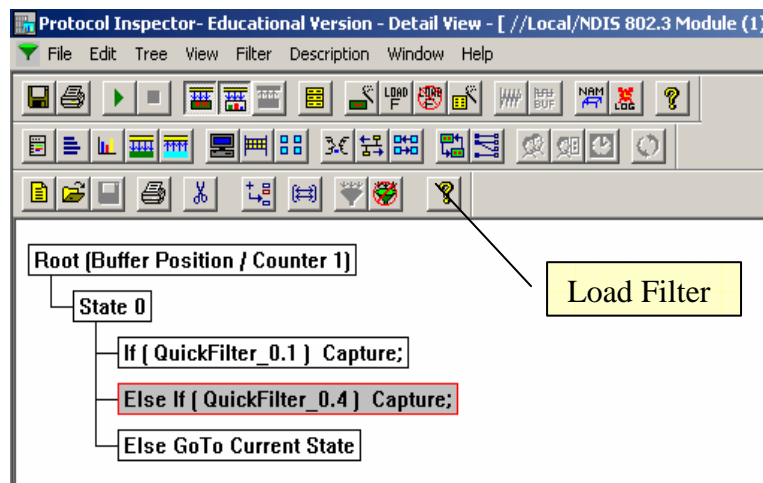



Figure 9.5

Do not close the window above, in order to keep the filter active.

Step 7. Go back to the first window, Protocol Inspector and start monitoring by pressing Start button ().

The monitor time should be a fixed period of time. To stop monitoring, press Stop button from Toolbar menu. The result is shown in the Monitor View window, in percents.

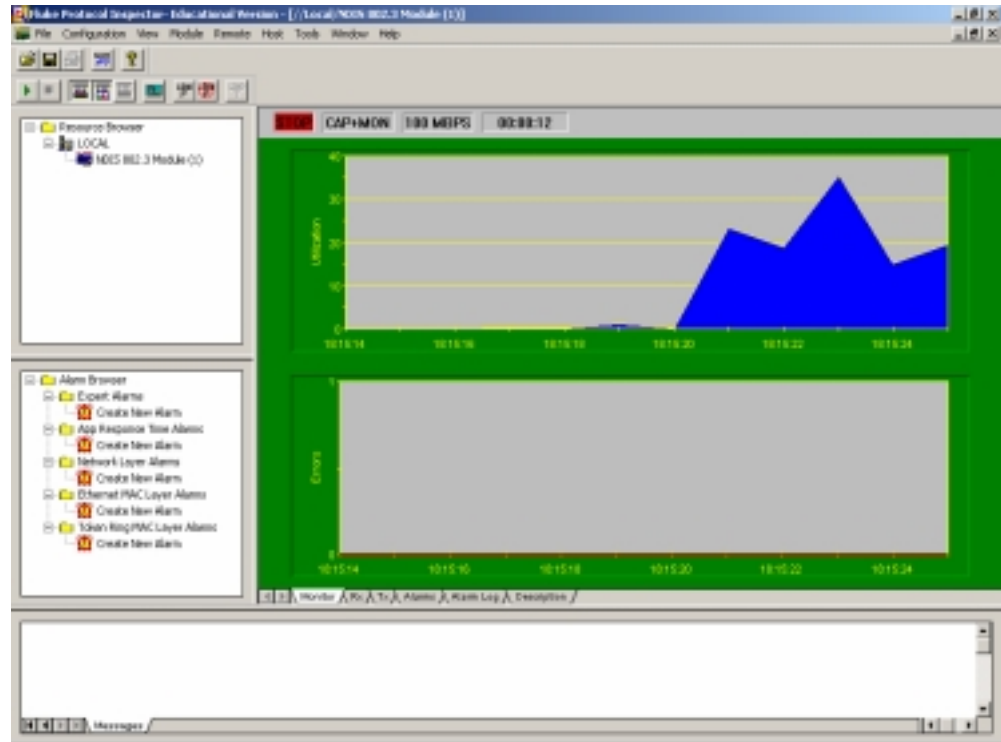



Figure 9.6

To see the packages captured press Capture View button (). The next picture shows the packages sent and received by KANT.

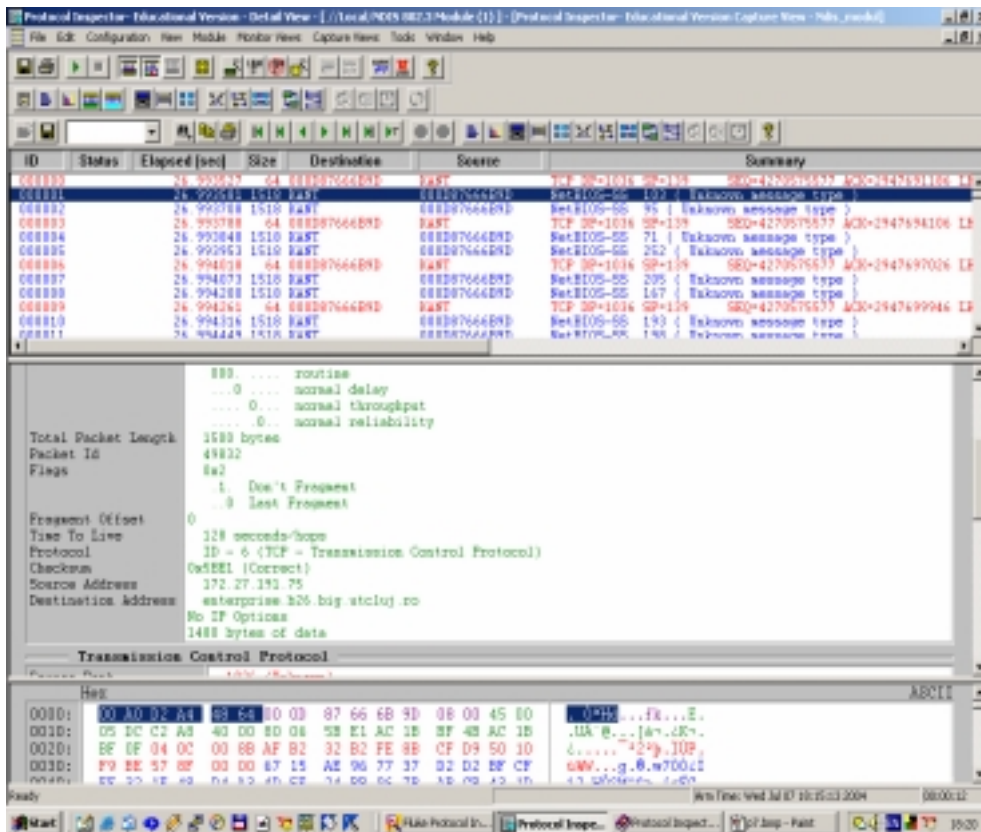



Figure 9.7

3. Lab activity

3.1 Open Protocol Inspector (Start->Programs->Fluke Networks-> Optiview

Protocol Expert EDV-> Optiview Protocol Expert EDV ).

3.2 Double click on the Monitor View or choose Module -> Detail View (F9) from the menu.

3.3 Select Module -> Capture Filter -> Create / Modify Capture Filter from the menu.

3.4 Open the window for selecting the conditions for filtering.

3.5 There must be built a filter to monitor the traffic between the current station and another station from the same class room.

Add the filtering conditions by pressing Add Condition button. Double click on the condition, for editing it, resulting condition edit window.

Note: For building filters in Optiview Protocol Expert EDV 5.0.2 there must be used templates. A filter is made up of more templates combined with logical operands. A condition must be added in the Add Conversation to Filter Template, and then saved. The filter is built after adding the templates in the Template Combination area.

3.6 Load the filter, in order to be active. Press Load Filer button from Toolbar Menu.

3.7 Go back to the first window, Protocol Inspector and start monitoring by pressing Start button

3.8 Run `ping` between the 2 stations using different parameters (different size packages) and stop monitoring, after the command is done.

3.9 Press Capture View button from Toolbar Menu to see the packages contains

If there is any FTP server installed, repeat all the steps above for files transfer, instead of `ping` command.

It's recommended to read the help provided by OPV-PE Fluke Networks, regarding to filters and creating new filters with different parameters.

Notes