LUCRAREA NR. 9
PROTOCOL INSPECTOR – UTILIZAREA FILTRELOR DE CAPTURĂ

1. Obiective

Obiectivul acestei lucrări este utilizarea avansată a Fluke Networks Protocol Inspector. Se va arăta modul în care se stabilesc filtrele pentru anumite protocoale şi anumite adrese (explicarea detaliată a creării sau modificării filtrelor de captură).

2. Consideraţii teortice

2.1 Introducere

Fluke Networks' OPV-PE este un program ce rulează sub Windows (2k, NT 4.x, XP). Acesta este o aplicaţie de analiză şi monitorizare a reţelelor Ethernet 10/100/1000.

Interfaţa sa utilizator furnizează o vizualizare cuprinzătoare a reţelei precum şi abilitatea de a analiza în adâncime la un segment specific al reţelei. Fereastra principală asigură o singură vizualizare utilizator pentru fiecare segment monitorizat.

OPV-PE se interfaţează în mod obişnuit cu una sau mai multe unelte de analiză hardware furnizate de Fluke Networks. OPV-PE poate simultan captura, monitoriza şi analiza dispozitive multiple cât şi a analiza datele capturate. De asemenea poate monitoriza segmentele reţelei locale; opţional software-ul la distanta îi permite programului Fluke Networks să comunice cu componente hardware Fluke Networks şi să acceseze produse Fluke Networs pe segmente la distanţă.

Lucrarea de laborator se bazează pe cunoaşterea noţiunilor de bază legate de modul de utilizare a programului Protocol Inspector prezentată în lucrarea de laborator de la materia „Reţele Locale de Calculatoare”.

2.2 Filtre

Cu ajutorul Protocol Inspector, se pot realiza capturi de pachete, prin folosirea filtrelor de captură. Filtrele de captură reprezintă o modalitate de vizualizare doar a pachetelor care respecta o anumită condiție, legată fie de sursă, fie de destinație. Astfel se pot vizualiza pachetele care vin spre o stație de lucru, server, sau pachetele care pleacă, sau chiar ambele variante. De fapt se poate monitoriza traficul în întreaga rețea de calculatoare, prin specificarea adresei MAC sau a IP-ului.

În lucrarea de față se va exemplifica folosirea acestor filtre pentru capturarea pachetelor primite şi trimise de către un sistem, cel pe care este instalat Protocol Inspector.

2.3 Definirea filtrelor

Se poate defini un filtru simplu folosind un şablon de filtru. Există două tipuri de şabloane de filtre:

- filtre şablon predefinite: urmăresc un anume tipar de date sau colecție de date. Filtrele predefinite sunt oferite de OPV-PE şi nu pot fi modificate.
- filtre şablon utilizator: urmăreşte de asemenea date specifice sau o colecție de date. Se poate construi un filtru utilizator, pe baza unor filtre predefinite sau prin specificarea directă a tiparelor datelor.

Cel mai folosit filtru utilizator este bazat pe un şablon predefinit şi adaugă un număr de conversație sau port. Se poat adăuga valori la offsetul pachetelor în formă hexazecimală, zecimală sau ASCII. O dată creat şi salvat, filtrul poate fi accesat de la căsuța Available Filter Templates.

O conversație este un şablon de date specifice adreselor sursă şi destinație, inclusiv tipul protocolului şi direcția traficului. Zona “Add Conversation to Filter Template” din fereastră asigură un mijloc facil de adăugare a adreselor la un filtru utilizator.

Un port este un şablon de date specifice numerelor port ale sursei şi destinației, inclusiv tipul protocolului şi direcția traficului. Zona “Add Port to Filter Template” din fereastră asigură un mijloc facil de adăugare a numerelor port la un filtru utilizator.

2.4 Utilizarea programului Protocol Inspector pentru definirea de filtre de captură

Pas 1. Se deschide Protocol Inspector (Start->Programs->Fluke Networks-> Optiview Protocol Expert EDV-> Optiview Protocol Expert EDV)

Pas 2. Se efectuează dublu click pe diagrama de monitorizare sau din meniu se alege Module -> Detail View (F9).

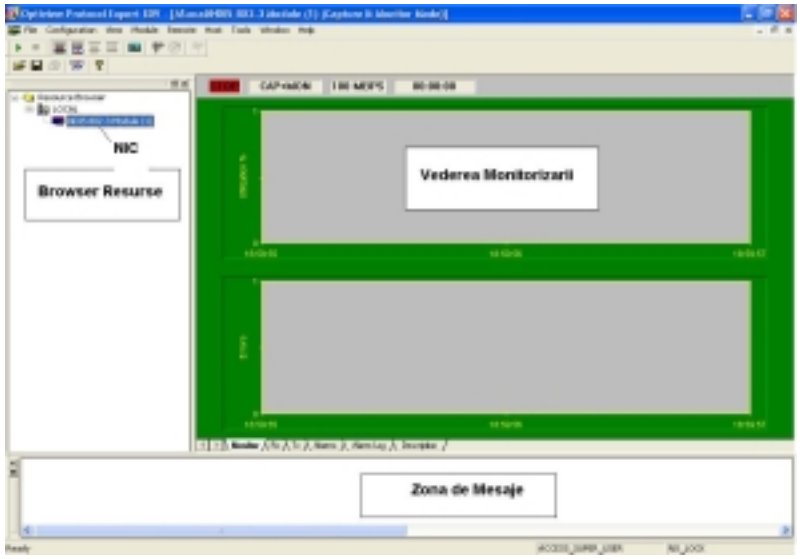
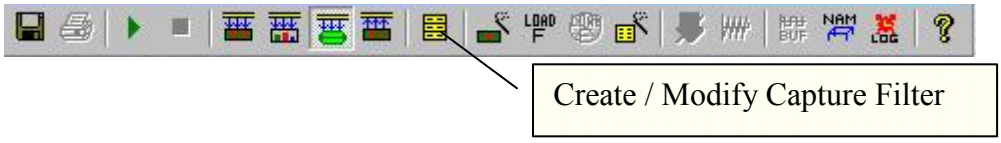


Figura 9.1

Pas 3. Se selectează din meniul Module -> Capture Filter -> Create / Modify Capture Filter.



Pas 4. Se va deschide fereastra de selecție a condițiilor de filtrare.

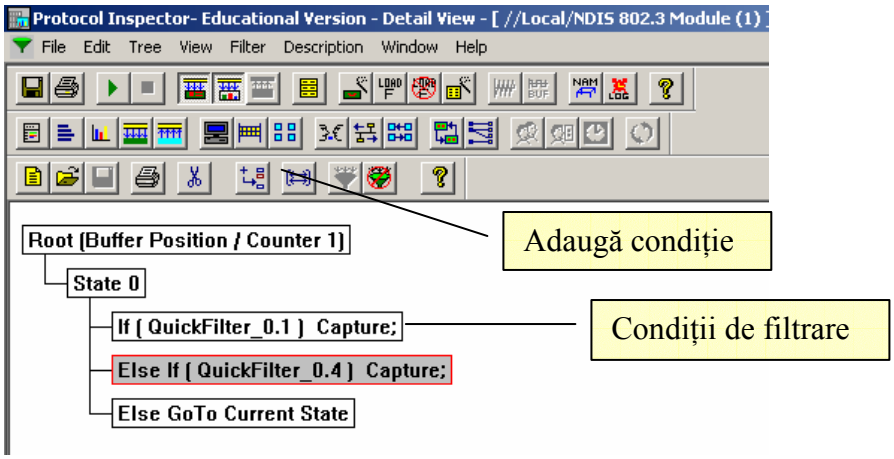


Figura 9.2

Pas 5. Se adaugă un număr de condiții de filtrare prin apăsarea butonului de adăugare condiții, iar pentru editarea lor, se efectuează dublu click pe fiecare condiție în parte, afișându-se fereastra de editare condiții.

În exemplul de mai jos, se filtrează toate pachetele care sunt primite de către stația KANT (în cazul de față)

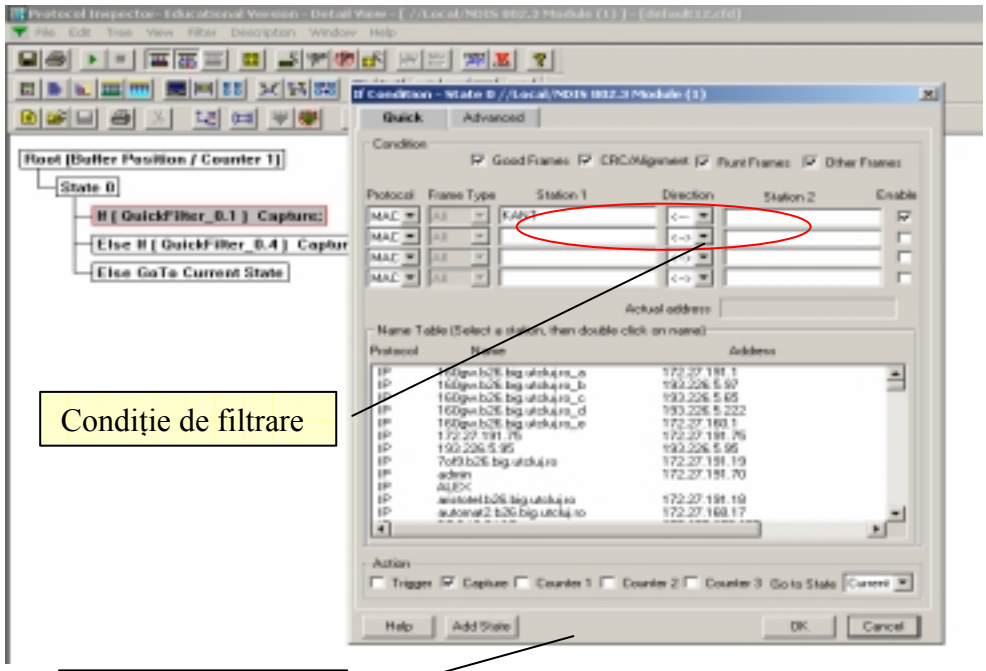


Figura 9.3

Pentru a realiza filtrarea se specifică din lista de calculatoare existente în rețea, IP-ul calculatorului dorit (sau MAC-ul) şi sensul de transmitere a pachetelor care urmează a fi capturate. Sensul poate fi unidirecțional sau bidirecțional, reprezentat prin săgeată (eventual dublă) către stațiile sursă sau destinație (< - >).
Pentru validarea condițiilor alese se continuă cu apăsarea butonului OK.

Pentru versiunea Protocol Inspector 5.0.2 fereastra de filtrare este prezentată în figura următoare.

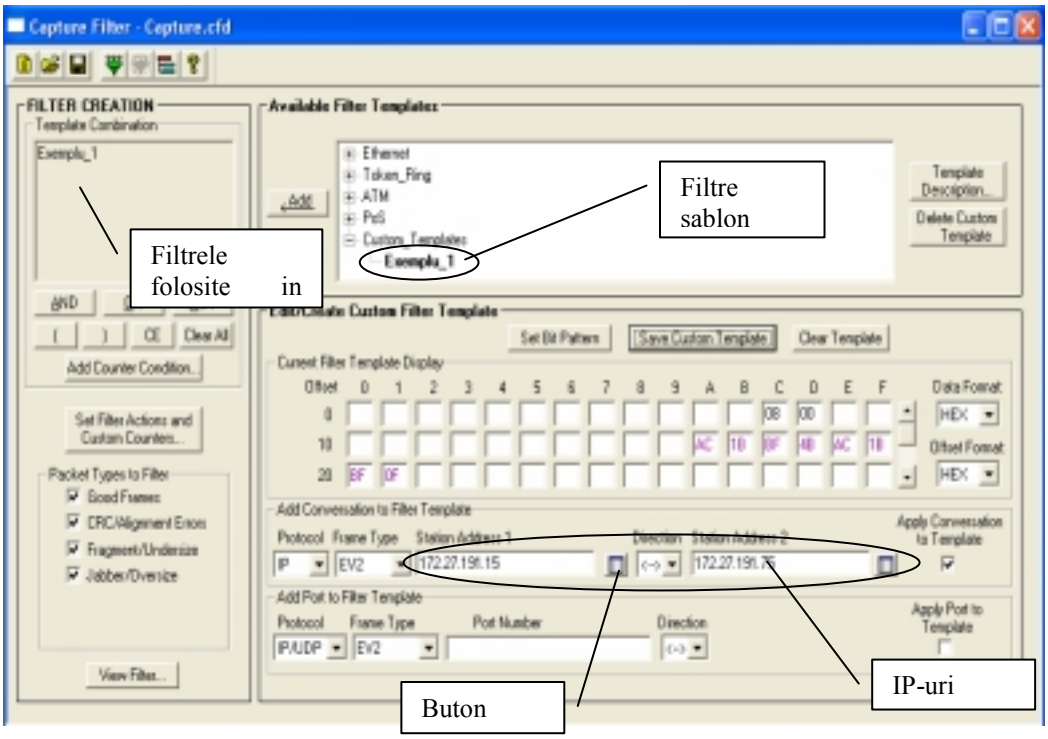


Figura 9.4

O conversație asigură un mod uşor de adăugare a adreselor la un filtru. Specificarea conversațiilor se realizează prin completarea secțiunii Add Conversation to Filter Template din cadrul ferestrei Capture Filter. Această secțiune a ferestrei este compusă din selectarea protocolul folosit, a tipului de cadre, adresele celor 2 stații de lucru, indicatorului de direcție şi a căsuței de selectare activare/dezactivare.

Tabelul 9.1

Protocol	MAC, IP, IPX sau Atalk (AppleTalk)
Tipul cadrelor	EV2 (EthernetII), SNAP, 8022 (IEEE 802.2), 8023 (IEEE 802.3), ISL, VLAN. Tipul cadrelor se aplică doar asupra adreselor IP
Adresa stației 1	Adresa completa IP, IPX, MAC sau ATalk a statiei
Traffic Direction Indicator	<-> Se capturează/afişează întregul trafic între stația 1 şi stația 2
	-> Se capturează/afişează întregul trafic unde stația 1 este adresa sursă şi stația 2 este adresa destinație
	<- Se capturează/afişează întregul trafic unde stația 2 este adresa sursă şi stația 1 este adresa destinație
Adresa stației 2	Adresa completa IP, IPX, MAC sau ATalk a statiei

Căsuța de selectare "Apply Conversation to Template" activează sau dezactivează o conversație ca parte a unui filtru şablon.

Protocolul şi tipul cadrelor sunt selectate din liste de selecție. OPV-PE restricționează automat utilizarea de combinații fără sens. OPV-PE va seta în mod automat protocolul corect şi tipul cadrelor când se selectează adresa unei stații din lista de nume.

Adresa stației poate fi scrisă direct în câmpul de adresă (Station Address) sau prin selectarea adresei din lista de nume. Prin apăsarea butonului Nume (Name) apare lista de nume curente pentru selectarea adresei. Fereastra de nume (Name Table) afişează toate numele şi adresele asociate, inclusiv protocolul tipul cadrelor. Numele şi adresele asociate sunt cele curent active în lista de nume. Prin dublu click pe un nume din tabelă, se încarcă numele în câmpul de adresă a stației. Dacă nu este specificată nici o adresă în câmpul de adresă, toate stațiile sunt capturate. De exemplu, daca se setează o adresă pentru stația 1, nici o adresă pentru stația 2 şi direcția ->, toate pachetele care au ca sursă stația 1 sunt capturate, indiferent de destinație. La specificarea adreselor pentru capturarea datelor de pe mai multe stații se pot folosi măşti. Se foloseşte caracterul X pentru a specifica orice valoare pe acea poziție. De exemplu, 343F4AXXXXXX pentru adresa fizică.

Pentru a aplica o conversație la filtrul şablon se selectează căsuța de selecție "Apply Conversation to Template". Prin aceasta este definită o singură conversație. Dacă se dorește folosirea unor conversații adiționale, trebuie create filtre avansate, sau folosirea măştilor, mai sus descrise. După crearea unui şablon (template) acesta se va adăuga cu butonul Add în zona Template Combination (unde se pot crea şabloane compuse între diferite conversații pentru a obține diferite filtre avansate).

Pas 6. Pentru activarea filtrului este necesară încărcarea acestuia, operație care se efecțuează prin apăsarea butonului  din Toolbar .

Observație: Înainte de încărcarea filtrului este recomandată salvarea acestuia. Operația de salvare se face prin apăsarea butonului 

din Toolbar.

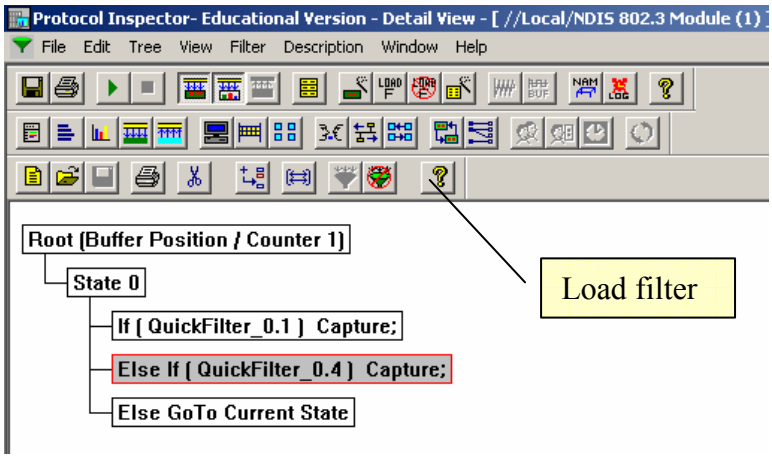


Figura 9.5

Pentru a păstra filtrul activ, fereastra de mai sus nu se închide.

Pas 7. Se revine în fereastra inițială a Protocol Inspector şi se porneşte monitorizarea prin apăsarea butonului Start 

Monitorizarea se face pe o perioadă determinată de timp după care se apasă butonul Stop pentru oprirea acesteia. Rezultatul monitorizării este afişat în fereastra de vedere a monitorizării sub formă de procente.

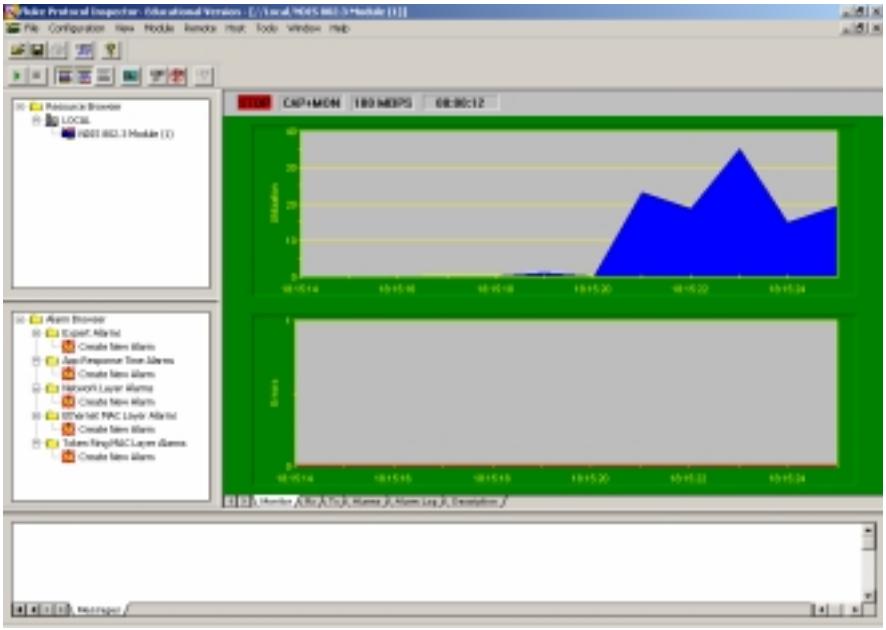


Figura 9.6

Pentru a vedea pachetele capturate se apasă butonul Capture View ()
Rezultatul capturii pentru stația KANT (pachetele primite şi trimise).

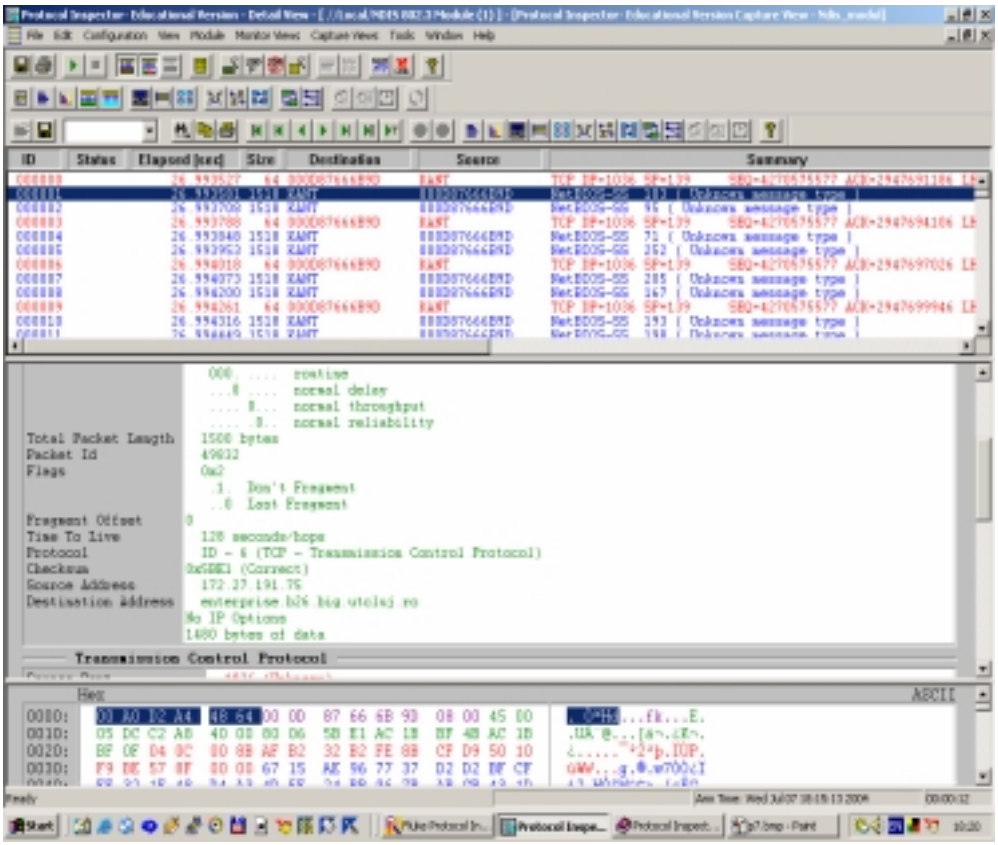


Figura 9.7

3. Desfăşurarea lucrării

Pas 1. Se deschide Protocol Inspector (Start->Programs->Fluke Networks-> Optiview Protocol Expert EDV-> Optiview Protocol Expert EDV).

Pas 2. Se efectuează dublu click pe diagrama de monitorizare (pentru vedere detaliată)sau din meniu se alege Module -> Detail View (F9).

Pas 3. Se selectează din meniul Module -> Capture Filter -> Create / Modify Capture Filter.

Pas 4. Se va deschide fereastra de selecție a condițiilor de filtrare.

Pas 5. Se va urmări traficul între stația de lucru curentă şi o altă stație din

rețea (preferabil din aceeaşi sală).
Se adaugă un număr de condiții de filtrare (adresele IP şi sensul de filtrare) prin apăsarea butonului de adăugare condiții, iar pentru editarea lor, se efectuează dublu click pe fiecare condiție în parte, afişându-se fereastra de editare condiții.

Observație: Pentru versiunea Optiview Protocol Expert EDV 5.0.2 filtrele se construiesc diferit prin utilizarea şabloanelor. Un filtru poate conține mai multe şabloane utilizate expresii logice care definesc filtrul. O condiție se adaugă în secțiunea Add Conversation to Filter Template, urmând a se salva. Pentru a construi filtrul se adăugă şabloanelor dorite în secțiunea Template Combination.

Pas 6. Pentru activarea filtrului este necesară încărcarea acestuia (Load Filter), operație care se efectuează prin apăsarea butonului din Toolbar.

Pas 7. Se revine în fereastra inițială a Protocol Inspector şi se porneşte monitorizarea prin apăsarea butonului Start.

Pas 8. Se dă comanda `ping` între cele 2 stații cu diverşi parametri (pachete de diverse mărimi) şi după terminarea execuției comenzii se opreşte monitorizarea.

Pas 9. Pentru vizualizarea conținutului pachetelor se selectează butonul Capture View din Toolbar.

Dacă este instalat un server FTP pe unul din calculatoare se poate repeta mersul lucrării de laborator cu un transfer de fişiere în loc de comanda `ping.`

Se recomandă citirea help-ului distribuit cu OPV-PE Fluke Networks, legat de filtre şi încercarea de a crea filtre noi cu alți parametri (condiții compuse).

Notițe