

Configurar filtros de Captura e Exibição

Última revisão feita em 02 de Julho de 2007.

Monitorar e analisar o tráfego da rede é tarefa necessária de um analista ou administrador para que eventuais problemas sejam evitados ou solucionados, não só como uma atitude reativa, mas também como uma posição pró-ativa. Utilizar o Network Monitor é uma das mediadas a serem tomadas como boa prática. A seguir você poderá acompanhar um artigo básico de utilização sem detalhes específicos e que servirá de guia para processos mais detalhados que você venha efetuar no seu dia-a-dia.

1. Configurando um filtro de captura (Capture Filter)

Para configurar um filtro de captura é só clicar no menu Capture > Filter ou apertar a tecla F8 no teclado.

Na janela Capture Filter você poderá configurar um filtro de acordo com o que precisar, basta selecionar uma das linhas na árvore apresentada. Perceba que você pode salvar (Save) o filtro que acabou de criar e também pode carregar (Load) um filtro existente.

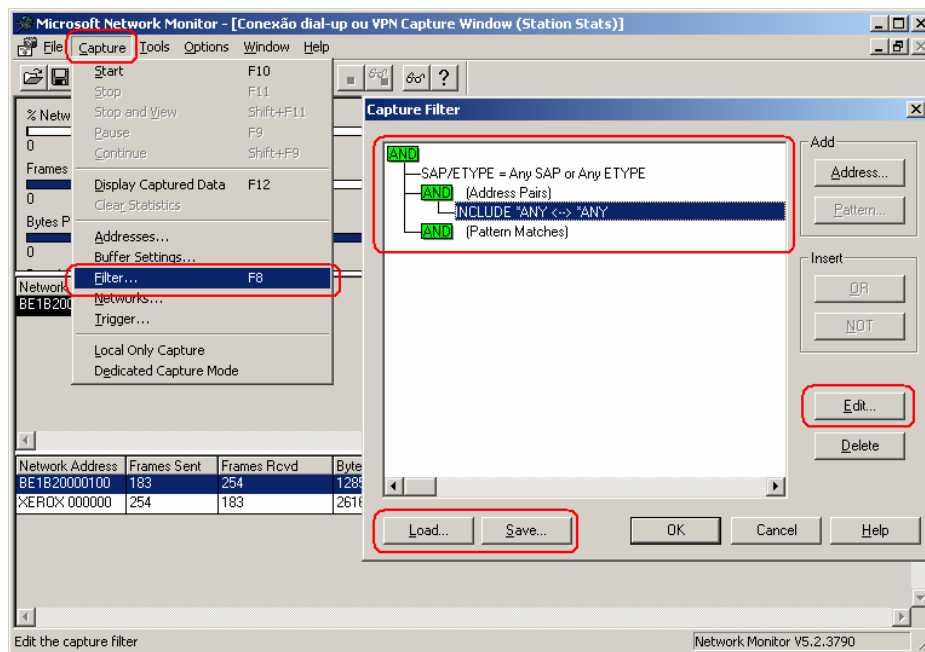


Figura 1.1 – Configuração básica de um filtro de captura.

Filtrando o tráfego por Protocolo

Selecionando a linha SAP/ETYPE e clicando no botão Edit você pode configurar o protocolo (ou os protocolos) que será (serão) monitorado (s) durante o processo de captura, habilitando ou desabilitando qual desejar.

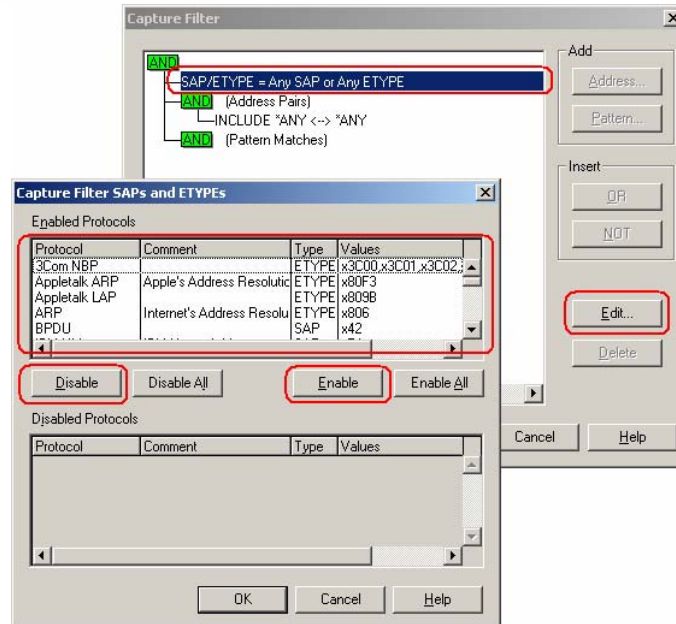


Figura 1.2 – Escolhendo o protocolo que fará parte do filtro atual.

Filtrando o tráfego por Endereço

Em seguida você poderá escolher o par de endereços que deverão ser analisados durante sua pesquisa. (É possível monitorar até quatro pares de endereços simultaneamente).

Um par de endereços consiste em:

- Endereços dos dois computadores cujo tráfego você deseja monitorar.
- Setas que especificam a direção do tráfego que você deseja monitorar.
- A palavra-chave INCLUDE ou EXCLUDE, que indicam como o Network Monitor deve responder a um quadro que atende às especificações de um filtro.

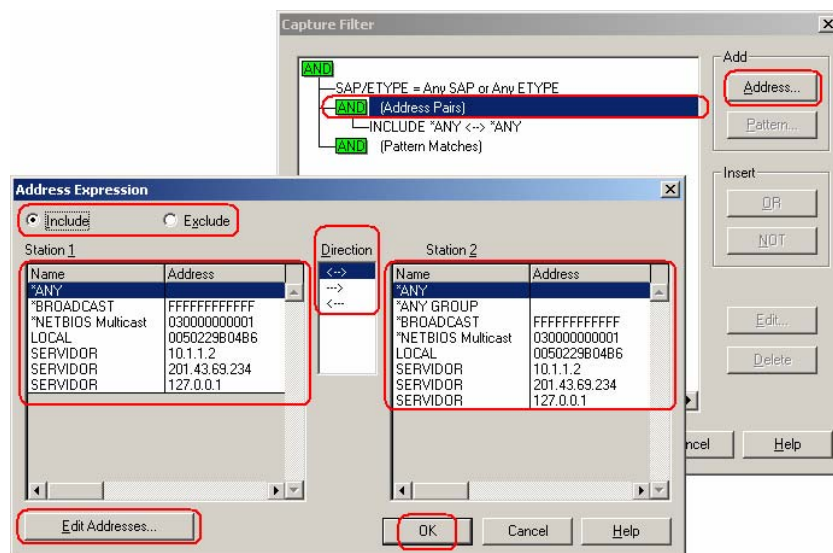


Figura 1.3 – Endereços dos computadores que serão monitorados.

Obs.: Independentemente da seqüência que as instruções aparecem na tela Capture Filter, as instruções EXCLUDE são avaliadas primeiro.

Filtrando o tráfego por Padrão de Dados

Neste caso você poderá limitar a captura aos frames que contenham um padrão específico de dados hexadecimais ou ASCII e também configurar para que a captura comece a partir de certo ponto do frame, especificando quantos bytes deverão ser ignorados antes de começar a pesquisa.

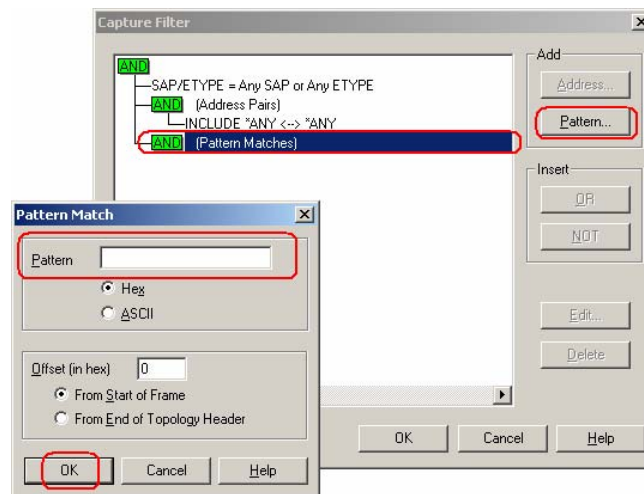


Figura 1.4 – Se necessário forneça um padrão hexadecimal ou ASCII.

2. Capturando o tráfego da rede

Depois de configurar o filtro da forma que melhor atende a sua necessidade é hora de capturar o tráfego desejado. No menu da ferramenta clique em Capture > Start.

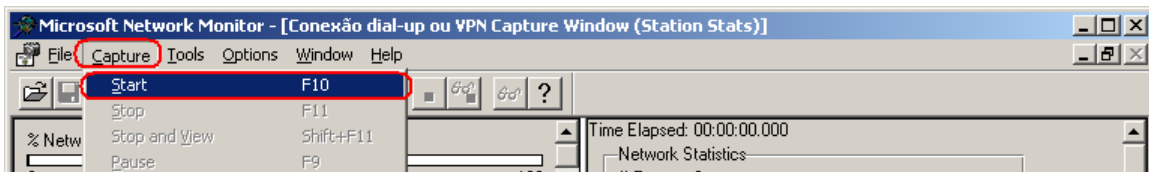


Figura 2.1 – Para iniciar a captura do frames clique na opção Start.

Obs.: Lembre-se que a captura atual fica armazenada num arquivo temporário no buffer, porem você pode salvar a captura para analisar posteriormente e realizar outra captura. Para salvar a captura atual é só seguir no menu File > Save as ou ao tentar executar uma nova captura você será questionado se quer salvar a captura atual.

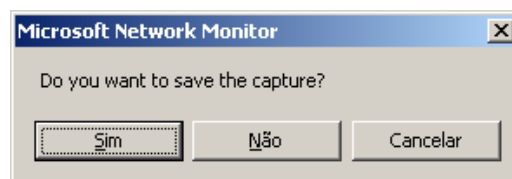


Figura 2.2 – É possível salvar as estatísticas da captura atual.

Uma explicação básica sobre os painéis da tela principal da ferramenta pode ser encontrada no artigo [Network Monitor - Visão Geral](#).

3. Visualizando o tráfego capturado

Quando a captura já for a ideal para análise você poderá dar o próximo passo, veja a seguir algumas das possibilidades:

- Parar a captura: acesse Capture > Stop (ou aperte F11).
- Parar e visualizar a captura: acesse Capture > Stop and View (ou aperte Shift+F11).
- Pausar a captura: acesse Capture > Pause (ou aperte F9).
- Limpar o buffer com a captura atual: acesse Capture > Clear_Statistics.

Obs.: Com a captura parada você pode voltar ao menu Capture e visualizar o resultado a qualquer momento (Capture > Display Captured Data), caso tenha apenas pausado a captura no mesmo menu você poderá continuar a captura (Capture > Continue).

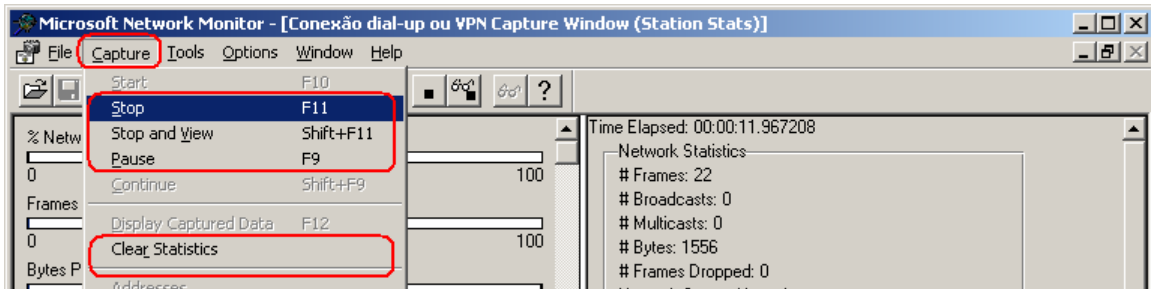


Figura 3.1 – Pare e continue o processo de captura quando quiser.

A tela a seguir mostra os dados de uma captura:

A screenshot of the Microsoft Network Monitor application window showing a list of captured frames. The title bar reads "Microsoft Network Monitor - [Capture: 3 (Summary)]". The menu bar includes "File", "Edit", "Display", "Tools", "Options", "Window", and "Help". The main area displays a table with the following columns: "Frame", "Time", "Src MAC Addr", "Dst MAC Addr", "Protocol", and "Description". The table contains 26 rows of data. The first row is highlighted. The status bar at the bottom shows "Network Monitor V5.2.3790", "F#: 1/880", "Off: 0(x0)", and "L: 0(x0)".

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description
1	0.060984	XER0X 000000	BE1B20000200	ICMP	Echo: From 201.43.69.234 To 201.50.184.146
2	0.064997	BE1B20000200	XER0X 000000	TCP	Control Bits: .A...., len: 0, seq: 7076...
3	0.064997	XER0X 000000	BE1B20000200	TCP	Control Bits: .A...., len: 1432, seq: 159438...
4	0.064997	XER0X 000000	BE1B20000200	TCP	Control Bits: .AP...., len: 1432, seq: 159438...
5	0.071016	BE1B20000200	XER0X 000000	ICMP	Time Exceeded: 201.50.184.146 (See frame 1)
6	0.071016	XER0X 000000	BE1B20000200	ICMP	Echo: From 201.43.69.234 To 201.50.184.146
7	0.112147	BE1B20000200	XER0X 000000	TCP	Control Bits: .A...., len: 0, seq: 340994...
8	0.119170	BE1B20000200	XER0X 000000	ICMP	Time Exceeded: 201.50.184.146 (See frame 6)
9	0.168326	BE1B20000200	XER0X 000000	TCP	Control Bits: .A...., len: 0, seq: 7076...
10	0.168326	XER0X 000000	BE1B20000200	TCP	Control Bits: .A...., len: 1432, seq: 159438...
11	0.168326	XER0X 000000	BE1B20000200	TCP	Control Bits: .AP...., len: 1432, seq: 159438...
12	0.209458	XER0X 000000	BE1B20000200	ICMP	Echo: From 201.43.69.234 To 201.50.184.146
13	0.222499	BE1B20000200	XER0X 000000	ICMP	Time Exceeded: 201.50.184.146 (See frame 12)
14	0.252595	XER0X 000000	BE1B20000200	ICMP	Echo: From 201.43.69.234 To 201.50.184.146
15	0.266640	BE1B20000200	XER0X 000000	ICMP	Time Exceeded: 201.50.184.146 (See frame 14)
16	0.276672	BE1B20000200	XER0X 000000	TCP	Control Bits: .A...., len: 0, seq: 268165...
17	0.276672	XER0X 000000	BE1B20000200	TCP	Control Bits: .AP...., len: 1440, seq: 162982...
18	0.276672	XER0X 000000	BE1B20000200	TCP	Control Bits: .A...., len: 1440, seq: 162982...
19	0.280685	XER0X 000000	BE1B20000200	TCP	Control Bits: .A...., len: 1440, seq: 222662...
20	0.347899	BE1B20000200	XER0X 000000	TCP	Control Bits:S., len: 0, seq: 292499...
21	0.347899	XER0X 000000	BE1B20000200	TCP	Control Bits: .A.R., len: 0, seq: ...
22	0.366960	XER0X 000000	BE1B20000200	ICMP	Echo: From 201.43.69.234 To 201.50.184.146
23	0.380002	BE1B20000200	XER0X 000000	ICMP	Time Exceeded: 201.50.184.146 (See frame 22)
24	0.409094	XER0X 000000	BE1B20000200	ICMP	Echo: From 201.43.69.234 To 201.50.184.146
25	0.416117	BE1B20000200	XER0X 000000	TCP	Control Bits: .A...., len: 0, seq: 340994...
26	0.416117	XER0X 000000	BE1B20000200	TCP	Control Bits: .AP...., len: 1160, seq: 222662...

Figura 3.2 – Dados de uma captura apresentada no painel de exibição.

Clicando duas vezes com o mouse numa linha específica da captura você terá os dados divididos em três painéis, de cima para baixo:

Painel resumo: exibe a lista dos frames na ordem em que foram capturados.

Painel detalhe: exibe informações sobre o frame selecionado no momento no painel Resumo. Essas informações incluem alguns detalhes e os protocolos que foram usados para enviá-lo.

Painel Hexadecimal: Exibe o conteúdo do frame em hexadecimal e uma representação alfabética do seu conteúdo em modo ASCII

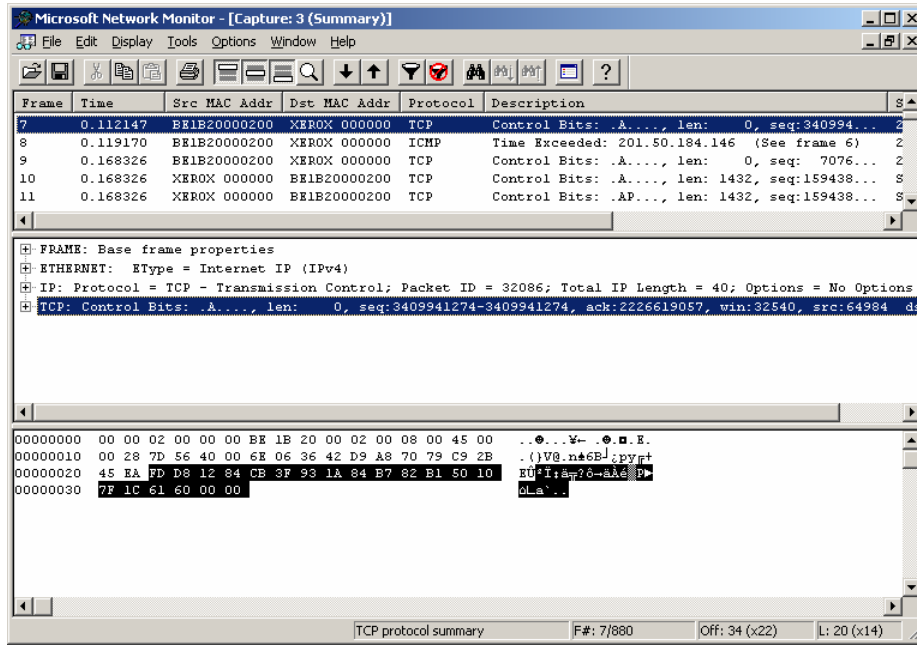


Figura 3.3 – O três painéis para análise da exibição dos dados.

Caso a captura tenha monitorado algo além do necessário para sua análise você pode criar um filtro de exibição (Display Filter) para organizar melhor o que você deseja ver. Para habilitar ou desabilitar um filtro de exibição acesse Display > Filter/Disable Filter.

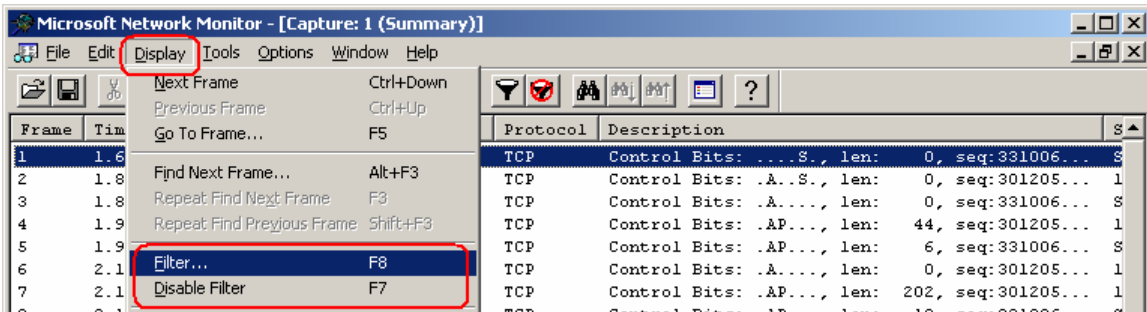


Figura 3.4 – Utilize um filtro de exibição para ajudar na análise dos dados coletados.

A tela de configuração de um filtro de exibição tem semelhanças com a tela para configuração de um filtro de captura. Você poderá filtrar os dados apresentados com base nos protocolos utilizados, em uma propriedade específica de algum protocolo ou ainda por endereço IP de algum computador.

Durante a configuração deste filtro de exibição você vai se deparar com basicamente as duas telas a seguir, veja:

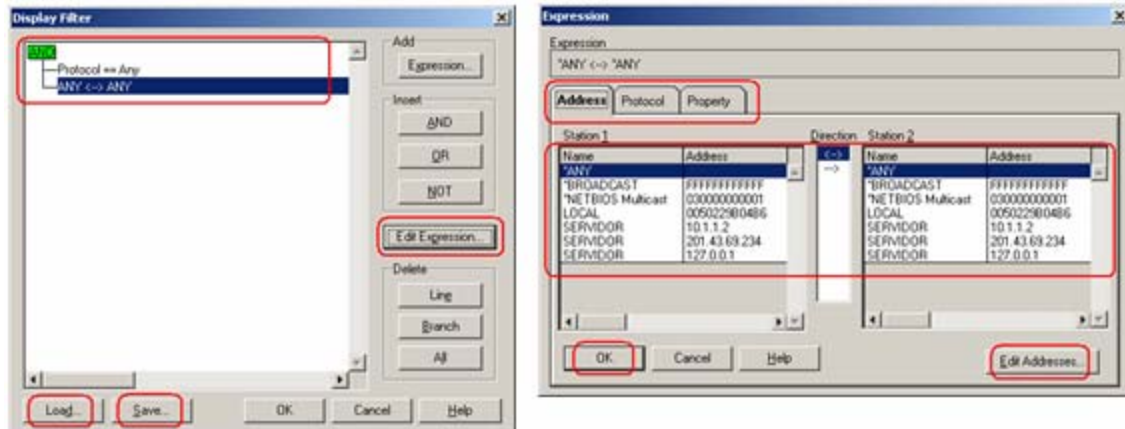


Figura 3.5 e 3.6 – Um filtro de exibição tem algumas semelhanças com o filtro de captura.

4. Melhores práticas de utilização

O ideal é utilizar o Network Monitor por períodos curtos de tempo, pois assim você evitará perda de desempenho no computador. Defina bem os filtros, tanto de captura quanto de exibição para que você analise a menor quantidade possível de dados, sendo assim colete apenas o que lhe for necessário para possibilitar um diagnóstico eventualmente mais rápido.

Os adaptadores Token Ring rejeitam frames maiores do que o tamanho especificado em suas configurações. Se você capturar frames em redes Token Ring, defina o adaptador de rede para aceitar o maior tamanho de frame Token Ring possível, de 17 KB. Consulte também a documentação de seu adaptador de rede.

Conclusão

Concluindo a leitura deste artigo você deve ter uma noção do que é necessário configurar para que uma captura de frames seja feita da melhor e mais simples forma utilizando o Netmon.

Bibliografia

Referências utilizadas na elaboração deste artigo:

1. Microsoft Brasil. www.microsoft.com.br
2. TechNet Brasil. www.technetbrasil.com.br

Escreveu,

Cleber Marques
contato@clebermarques.com

Segunda-feira, 02 de Julho de 2007.