

## Visão Geral

Última revisão feita em 29 de Junho de 2007.

Conheça o Network Monitor e entenda o quanto ele é útil na administração de uma rede.

### O que é o Netmon

O Network Monitor (Monitor de Rede), mais conhecido como Netmon, é uma ferramenta utilizada para capturar informações da rede para a identificação, análise e solução de eventuais problemas. O Netmon exibe através de sua interface as informações sobre o tráfego de rede capturado e, através destas informações, o administrador da rede poderá decidir o próximo passo na solução de um problema.

É importante lembrar que existem atualmente duas versões do Netmon: a versão básica (Lite) e a versão Completa (Full). A versão Lite você pode encontrar no Windows NT, 2000 e 2003, adicionando a ferramenta através da opção "Componentes do Windows", e contém apenas alguns recursos se comparada com a versão completa. Já a versão Full é distribuída com o Microsoft Systems Management Server (SMS).

A principal diferença entre as duas versões é que a Lite apenas captura o tráfego de rede que sai ou que é enviado ao computador em que ela está instalada, o conhecido to or from. Já a versão Full consegue capturar e exibir no modo to or from, e também todo e qualquer tráfego não criptografado de qualquer segmento da rede onde exista um desktop ou servidor com a versão Full instalada. Este modo é conhecido como Promiscuous mode e vai depender dos adaptadores de rede nos computadores, pois alguns modelos não suportam isso, mas são raros.

### Como funciona o Netmon

Ao instalar o Netmon em um computador, no caso da versão Lite, será possível capturar os pacotes que chegarem até o adaptador de rede deste computador através do tráfego na LAN. O Netmon poderá exibir ou salvar estes frames (como também são chamados) para análise posterior. Esta captura de pacotes pode conter regras e filtros como, por exemplo, capturar apenas os pacotes que venham de um determinado IP ou até mesmo que sejam de um determinado tipo de protocolo. É possível também criar alguns critérios de captura como iniciar ou parar um processo de captura a partir do momento que o Netmon detectar um conjunto específico de condições na rede (os chamados Triggers).

Existem filtros (Filters) de captura (Capture) e exibição (Display), os filtros de captura servem para que você especifique o que será capturado, retirando o excesso de informações e possibilitando que a análise seja feita de uma forma mais direta, sem contar que este filtro é aplicado em tempo real para o tráfego que está sendo monitorado. Já o filtro de exibição serve para filtrar dados já coletados, ou seja, este filtro é aplicado no tráfego já monitorado e serve para organizar melhor o que será analisado.

### Características

A principal característica do Netmon é monitorar o tráfego para/de um computador com a versão Lite instalada ou ainda monitorar o tráfego de um computador remoto com a versão Full (que vem com o SMS). Estes frames terão suas estatísticas apresentadas na tela do programa para análise.

A tela principal do programa possui quatro painéis e um menu, acompanhe a seguir como esta interface está organizada:

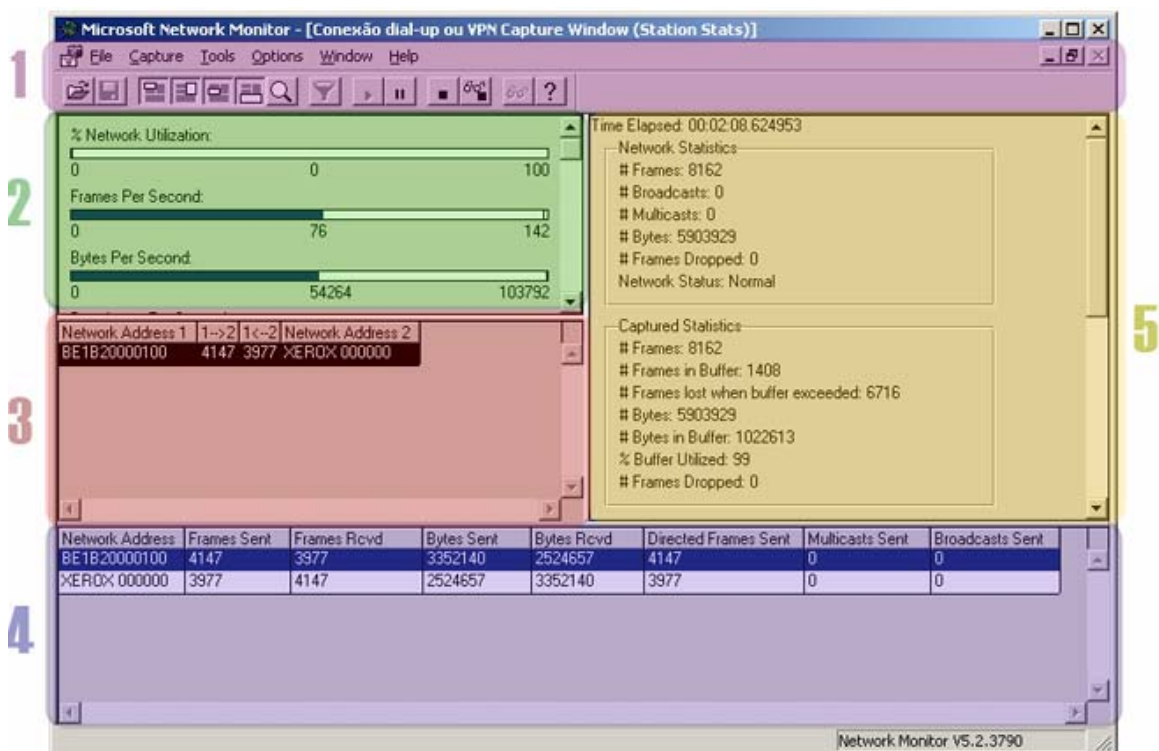


Figura 1.1 – O Network Monitor Lite, que acompanha o Windows.

1. Menu principal da ferramenta.
2. Este painel representa com um gráfico as estatísticas totais da captura atual.
3. Neste painel são exibidas as estatísticas para cada seção participante.
4. Resumo dos pacotes capturados desde o início do processo.
5. Estatísticas dos pacotes enviados de/para o computador com o Network Monitor.

## Os benefícios

Além de a ferramenta ser gratuita, por vir com o Windows no caso da versão Lite, o benefício maior é contar com mais um auxílio para um bom troubleshooting.

## Conclusão

Conhecer o Network Monitor é indispensável, saber como ele funciona e para que ele serve, agora o próximo passo é saber como instalar e analisar suas capturas. Até lá.

## Bibliografia

Referências utilizadas na elaboração deste artigo:

1. Microsoft Brasil. [www.microsoft.com.br](http://www.microsoft.com.br)
2. TechNet Brasil. [www.technetbrasil.com.br](http://www.technetbrasil.com.br)

Escreveu,

**Cleber Marques**  
[contato@clebermarques.com](mailto:contato@clebermarques.com)

Sexta-feira, 29 de Junho de 2007.