

S A F O - Sistema Agregador de Ferramentas de Operação de rede

... * †

CPGCC, Instituto de Informática, UFRGS
Caixa Postal 15064
91501-970 Porto Alegre - RS

Sumário

Este artigo apresenta o SAFO (Sistema Agregador de Ferramentas de Operação de rede), que é o resultado de um estudo de várias ferramentas já existentes e a seleção de um conjunto mínimo necessário para a realização de monitoração e manipulação dos componentes da rede. As ferramentas selecionadas foram integradas num único ambiente. Um tratamento é aplicado nas informações geradas pela execução das ferramentas, auxiliando na interpretação destes resultados e interagindo com um arquivo de recomendações, facilitando o uso das ferramentas e agilizando a tarefa dos operadores de rede.

Abstract

This article presents the SAFO (Integrate System of Tools for Network Operation), resulting from a study of many existing tools and from selection of a minimum set necessary for monitoring and network components handling. The select tools were integrated in an environment only. A treatment on information produced for tolls execution help on the interpretation of results and a interaction with a advices file will facilitate your use and will agilitate the network operator work.

1 Introdução

O gerenciamento de redes de computadores é bastante complexo, devido ao caráter distribuído dos elementos a monitorar e gerenciar. Muitas ferramentas tem sido desenvolvidas, para auscultar um ou outro aspecto da rede.

*Universidade Federal de Santa Maria, atualmente mestranda do CPGCC/UFRGS (.@inf.ufrgs.br).

†Universidade Federal do Rio Grande do Sul, Professora do CPGCC da UFRGS, (.@penta.ufrgs.br).

Para os que tem a incumbência desta tarefa, usualmente falta tempo para o estudo e teste de todas estas ferramentas e o resultado é que muitas ficam sem uso, apesar de valiosas. Por outro lado, apesar de existirem muitas ferramentas integradas, com suporte gráfico, tal como Sun Net Manager, HP Open View, IBM NetView existe um certo grau de impaciência por parte dos operadores de rede em navegar pelas telas gráficas destas ferramentas, devido ao desempenho nem sempre satisfatório, uma vez que as próprias estações de trabalho usadas são muitas vezes sub-dimensionadas para suportar aqueles programas. Assim, a modalidade ‘command line’ de algumas ferramentas de inspeção e controle da rede constituem a prática mais usual, como se pode observar, a partir de um levantamento efetuado e que cujos resultados estão comentados na sessão 2 deste trabalho.

A sintaxe e os parâmetros específicos inerentes a cada ferramenta muitas vezes inibem seu uso. Assim, foi iniciado um trabalho visando o projeto e implementação de um sistema que integrasse um conjunto mínimo destas ferramentas para que, o operador de rede pudesse utilizá-las de modo mais fácil, com uma interface mais amigável e com ‘helps’ embutidos. As ferramentas selecionadas foram integradas através de uma interface gráfica baseada nos sistemas XWINDOWS/XVIEW, possibilitando um fácil acesso ao ‘help’ e ao ‘assistant’ do sistema, bem como aos mais diversos parâmetros utilizados nas diferentes ferramentas. A inclusão de novas ferramentas (ou exclusão) é realizada facilmente, sem esforços de programação, tornando o sistema mais flexível. O tratamento dos resultados gerados pela execução das ferramentas e a interação com um arquivo de recomendações auxiliarão na interpretação dos resultados e na busca de possíveis soluções para os problemas de gerenciamento. O trabalho está em fase final de desenvolvimento e o resultado será colocado a disposição da comunidade (shareware).

SAFO-Sistema Agregador de Ferramentas de Operação de rede - destina-se a operadores de rede propiciando mecanismos para a monitoração e manipulação dos componentes da rede.

O estudo das ferramentas mais adequadas foi iniciado com as sugestões relacionadas no RFC1147 [STI 90]. Também foram usados e testados vários utilitários disponíveis em ambiente unix [SUN 90]. Para definir o conjunto mínimo, buscou-se subsídios junto a administradores de rede. O resultado desta análise está apresentado na sessão 2 deste trabalho. A seguir são relacionadas e brevemente comentadas as ferramentas selecionadas e por último é apresentado o sistema projetado.

2 Atividades típicas dos gerentes de rede

As redes de computadores tem um papel fundamental atualmente. Para cumprirem com seus objetivos necessitam estar em plenas condições de uso e para que isto aconteça, o gerenciamento é indispensável. As pessoas responsáveis pela administração da rede veêm-se diante de vários aspectos a gerenciar e inúmeras ferramentas disponíveis para auxiliar na tarefa, mas que geralmente são deixadas de lado por serem de difícil utilização, exigirem muito recurso de máquina, etc.

Para manter a rede operacional, os gerentes necessitam:

- **A) Monitorar o sistema**

A monitoração do sistema é um aspecto fundamental do gerenciamento de redes. É dividida em duas categorias: detecção de erro e monitoração básica (observação).

- **B) Detectar falhas e isolamento**

Quando o sistema falha, o gerente deve tentar diagnosticar a causa o mais rápido possível para o sistema retornar ao funcionamento normal.

- **C) Testar a performance**

O gerenciamento da performance tem duas atividades: monitoramento passivo do sistema, para detectar problemas e determinar seu perfil normal de operação, ou teste ativo da performance, com geração de tráfego artificial para avaliar a resposta dos recursos da rede.

- **D) Configurar o sistema**

Gerenciar a configuração é setar, coletar e armazenar o estado e os parâmetros dos recursos da rede.

Como o objetivo do SAFO é apresentar, num único ambiente integrado, as ferramentas mais utilizadas pelos administradores para atenderem suas necessidades de gerenciamento, foi realizada uma pesquisa junto a gerentes de rede, para conhecer quais as ferramentas que estavam sendo mais utilizadas diariamente. A pesquisa foi feita nas listas (nacional: REDES-L e internacional: BIGLAN). O resultado do levantamento se encontra resumido no quadro a seguir.

Resumo da Pesquisa

Ferramenta	Número de respostas	Porcentagem	A	B	C	D
ping	3	22	X	X	X	
tracert	3	22	X	X	X	
nslookup	2	14	X			
netstat	1	7	X	X		
etherfind	1	7	X	X	X	
rup	1	7	X	X		
ifconfig	1	7				X
tcpdump	1	7	X		X	
ps	1	7	X	X	X	

Alguns reportaram o uso de ferramentas integradas como: SunNetManager, NetView e HP Open View, principalmente os que gerenciam redes no exterior. Todas as ferramentas selecionadas serão brevemente apresentadas no próximo capítulo.

3 Ferramentas do Sistema SAFO

Fazem parte do SAFO dez ferramentas consideradas mais usuais, que são relacionadas a seguir com uma descrição sucinta de sua função .

Ping - Ping é uma das ferramentas básicas para gerenciamento na Internet. Verifica se um host, uma rede ou uma interface estão funcionais. Verificar se um dado componente

da rede esta ativo é uma das mais básicas atitudes de um gerente quando um problema ocorre. Portanto, a ferramenta que permite no mínimo realizar esta tarefa é imprescindível. Não foi surpresa pois verificar que é bastante usada. Oferece algumas variantes, como `-s`, que permitem facilitar todas as atividades referidas na sessão 2.

Traceroute - Permite obter a rota por pacote (nós visitados de uma origem até o destino). Pode ser usado para inspecionar situações onde o encaminhamento do pacote IP falhar, tal como quando um gateway intermediário descarta pacotes; ou implementações de IP intermediários que não suportam registro de rota. Mostra também o ‘round trip delay’ entre a origem e o gateway intermediário, para determinar a contribuição de gateways individuais para o delay end-to-end.

Nslookup - É um programa usado para consultar o nome ou endereço IP de máquinas num domínio Internet. Este programa é útil para diagnósticos de roteamento ou problemas de distribuição de mail, onde muitas vezes um servidor de domínio local está respondendo com um endereço Internet incorreto. Tem dois modos, interativo e não-interativo: O modo interativo permite ao usuário consultar informações (nome ou endereço IP) de vários hosts e domínios ou escrever a lista dos hosts no domínio; O modo não-interativo, escreve somente o nome e o endereço Internet de um host ou domínio consultado. Nslookup possui várias opções, que podem ser listadas com o help.

Netstat - Mostra o status da rede. Acessa a estrutura de dados da rede dentro do kernel e apresenta no vídeo em vários formatos.

Traffic - Mostra o tráfego ethernet graficamente em subjanelas, cada qual dando uma diferente visão do tráfego na rede. Pega as estatísticas do etherd (servidor de estatísticas ethernet), que deve estar rodando no host.

Etherfind - Examina os pacotes que atravessam a interface da rede e coloca num arquivo texto a descrição do tráfego. Pode gravar todo o tráfego de pacotes da ethernet ou o tráfego para um host local. As informações do arquivo são valores como tipo do protocolo, tamanho, origem e destino. Coloca a interface em modo promíscuo, exceto se utilizar a opção ‘-p’. O Etherfind pode filtrar os pacotes, com base nos protocolos (IP, ARP, RARP, ICMP, UDP, ND, TCP), ou baseado nos endereços de origem e destino, ou ainda nos números das portas TCP e UDP.

Ifconfig - Configura os parâmetros da interface da rede. É usado para associar um endereço a uma interface da rede e/ou para configurar os parâmetros da interface da rede. A configuração das interfaces e a verificação do seu estado, se estão ‘up’ ou ‘down’ é condição preliminar no gerenciamento de redes. O ifconfig, usado sem opções, mostra a configuração corrente para a interface da rede.

Rup - Mostra o status das máquinas locais. Faz um broadcast na rede local e mostra as respostas que recebe. Se o argumento ‘host’ é dado, o broadcast somente será realizado na lista de hosts especificados.

Tcpdump - Pode interpretar e escrever os cabeçalhos de vários protocolos como ethernet, IP, ICMP, TCP, UDP, NFS e outros. É útil para examinar e interpretar as retransmissões e operações de gerenciamento de implementações TCP. O arquivo de log gerado por ele contém, em cada linha de saída, a hora que o pacote foi recebido, tipo do pacote e outros valores do cabeçalho.

Ps - mostra o status dos processos correntes. Com os parâmetros é possível selecionar como e quais processos serão mostrados. Muito utilizado para verificar qual ou quais processos estão reduzindo a performance da máquina, se estão rodando, a quanto tempo e quanto de CPU estão consumindo.

4 Sistema SAFO

SAFO-Sistema Agregador de Ferramentas de Operação de rede é formado por um conjunto de módulos (ferramentas) independentes. Cada módulo do sistema realiza sua função e transmite seus resultados. Foram desenvolvidos vários programas fontes, que são chamados a partir do programa principal. Fazem parte da versão atual 70 arquivos, que ocupam aproximadamente 60 K. O sistema foi projetado para permitir o uso das ferramentas selecionadas de uma maneira mais ergonômica. Para alcançar tal meta, foi desenvolvido um protótipo que:

- integra, num sistema de janelas, as ferramentas selecionadas;
- oferece um conjunto de telas de help genérico (explicando a ferramenta em si) ou específico (explicando cada parâmetro e seu domínio ou escopo).
- possibilita a inclusão de novas ferramentas no sistema ou a retirada de alguma ferramenta que não se faz mais necessário.
- permite um tratamento sobre as informações geradas pela execução das ferramentas, auxiliando na interpretação das mesmas.
- interage com um arquivo de recomendações, facilitando a resolução do problema ocorrido.

A figura 1 mostra o esquema de funcionamento do SAFO.

4.1 Ambiente de Implementação do SAFO

O ambiente onde o protótipo está sendo implementado é composto por:

1. estação de trabalho do tipo SUN-SPARC
2. sistemas de janelas XWINDOWS/XVIEW
3. linguagem de programação C
4. sistema operacional UNIX

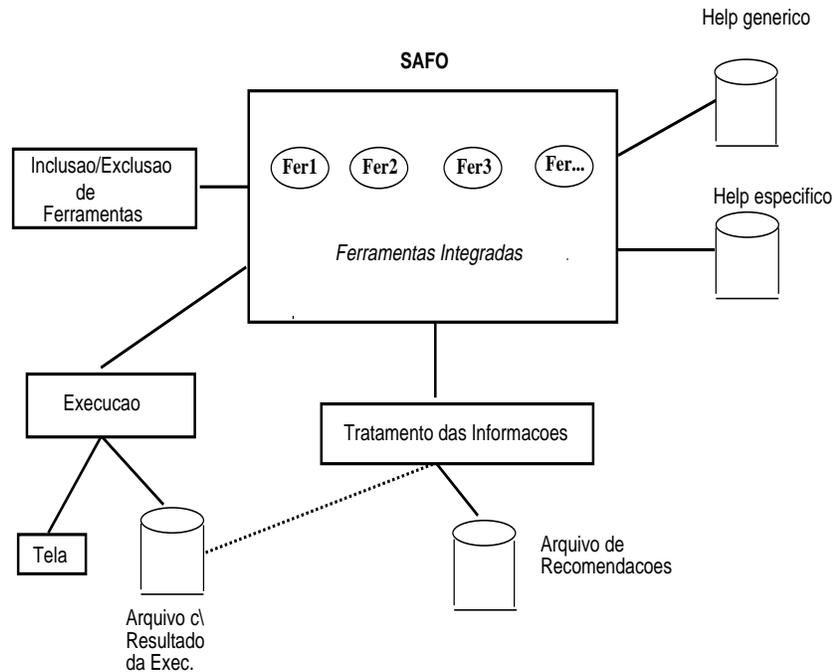


Figura 1: Funcionamento do SAFO

5. ferramenta de auxílio à criação de interfaces com o usuário.

A tarefa de projeto de uma interface é simplificada pelos gerenciadores disponíveis, que oferecem um conjunto consistente de funções, definições e normas de codificação .

A ferramenta geradora de interface com usuário utilizada no SAFO foi o GUIDE (Graphical User Interface Design Environment), versão 1.1, juntamente com o GXV, com a função de criar janelas, posicionar elementos, simular o funcionamento da interface.

Após a finalização da interface, é gerado o código em linguagem C que implementa esta interface. Com a consistência do código da interface com o usuário, com rotinas de notificação e eventos definidos, resta preencher o 'esqueleto' do código com o algoritmo da ferramenta.

4.2 Interface Gráfica e seu Funcionamento

A interface gráfica é a ferramenta que permite a entrada de comandos globais e a exibição de resultados.

4.2.1 Chamada do Sistema

Para iniciar a execução do sistema basta tornar o aplicativo disponível no menu de programas da workspace ou simplesmente escrever o nome do sistema em uma janela de shell. A linha de comando é mostrada a seguir:

```
lynx% SAFO
```

Imediatamente o sistema é carregado. Um croqui da janela principal é mostrado na figura 2, onde distinguem-se duas regiões:

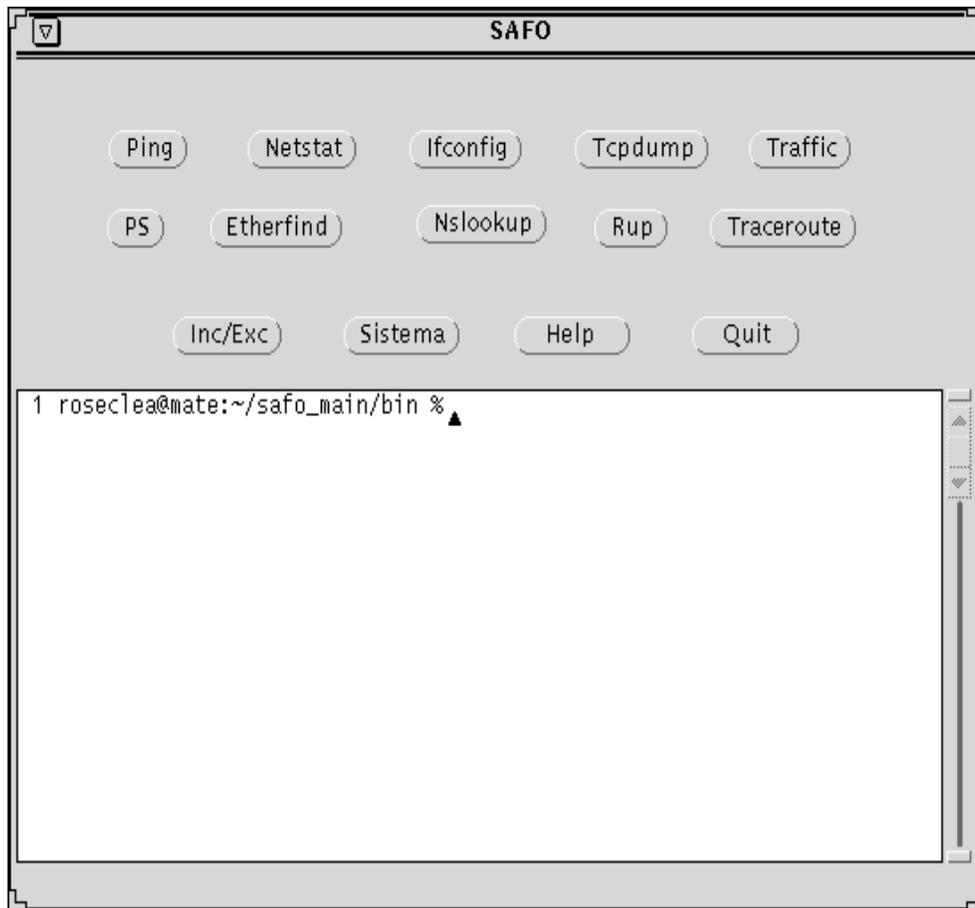


Figura 2: Interface SAFO

1. A região de visualização (superior) exibe através de botões todas as ferramentas disponíveis, permitindo assim uma visão geral das funções que podem ser executadas pelo sistema.
2. A região de resultados (segunda região) mostra os resultados decorrentes da execução das ferramentas.

Na região de visualização, além das ferramentas de gerenciamento são oferecidas as opções de encerramento do sistema (botão Quit), inclusão e exclusão de ferramentas (botão Inc/Exc), alteração de arquivos do sistema (botão Sistema) e de help do sistema, que pode ser de duas maneiras:

- botão HELP, que mostra um texto que explica a função de todas as ferramentas, de uma maneira geral. A figura 3 apresenta a tela de help das ferramentas.

No 'Help Text' é apresentado o nome da ferramenta e uma descrição sucinta do que ela realiza. Os nomes não estão listados em ordem alfabética e sim como estão posicionados na tela principal do sistema. Para recorrer todo o texto é utilizado a barra de scrolling vertical, posicionada a direita da janela.

- help de uma ferramenta específica, que apresenta texto descritivo somente desta. Cabe ressaltar que além de ler o texto de help, o usuário pode editá-lo, incluindo suas

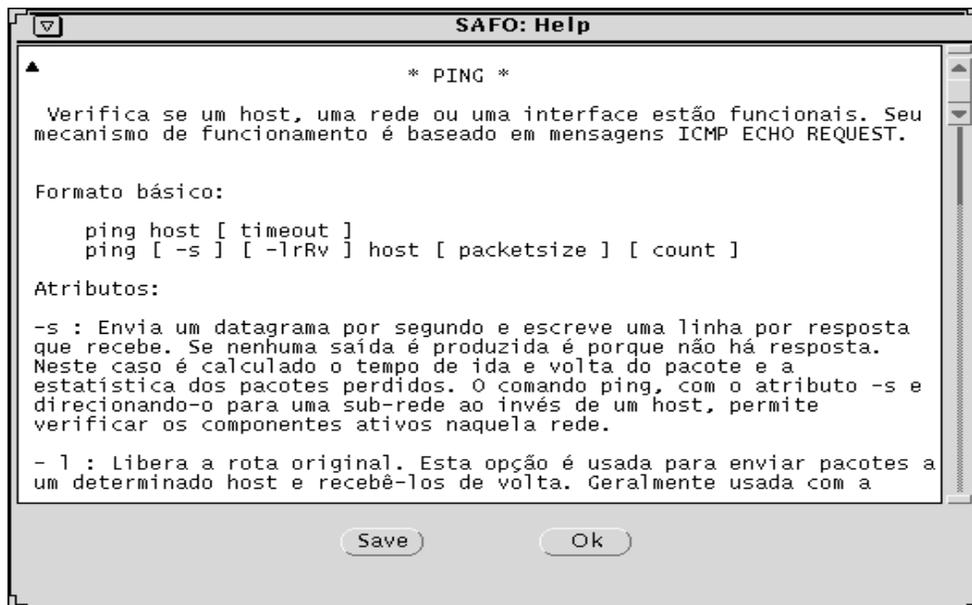


Figura 3: Help das Ferramentas do Sistema

próprias informações explicativas e observações que se fizerem necessárias, salvando o mesmo.

4.2.2 Execução

Ao escolher uma das ferramentas oferecidas, é apresentada uma janela para a entrada de parâmetros. Cada ferramenta tem o seu próprio conjunto de parâmetros, como já foi visto no capítulo 3. Como exemplo, vamos supor a escolha da ferramenta PING.

A figura 4 mostra uma janela ‘pop-up window’ com o nome da ferramenta no cabeçalho. As opções selecionadas vão direcionar a sua execução .

Após a escolha, deve ser feita a confirmação pressionando o botão ‘Apply’ ou o cancelamento/saída da operação com ‘Quit’. Nesta janela, o botão de ‘Help’ apresenta e explica todos os parâmetros possíveis para a ferramenta em questão.

Opções e Parâmetros default

Na maioria dos parâmetros, as opções foram criadas com tipo ‘Nonexclusive’, ou seja, torna possível setar várias opções para a mesma execução .

Foi determinada também uma opção ‘default’, onde o cursor se posiciona automaticamente ao abrir a janela (esta opção é a que será executada quando for pressionado o botão ‘select’ do mouse sem abrir a janela).

Host

O campo ‘Host’ permite entrada de nomes de hosts tanto na forma numérica (ex: 192.158.120.1) como alfabética (ex: lynx.uca.ufms.br).

Count

Neste campo será informado o número de vezes que o pacote será enviado.

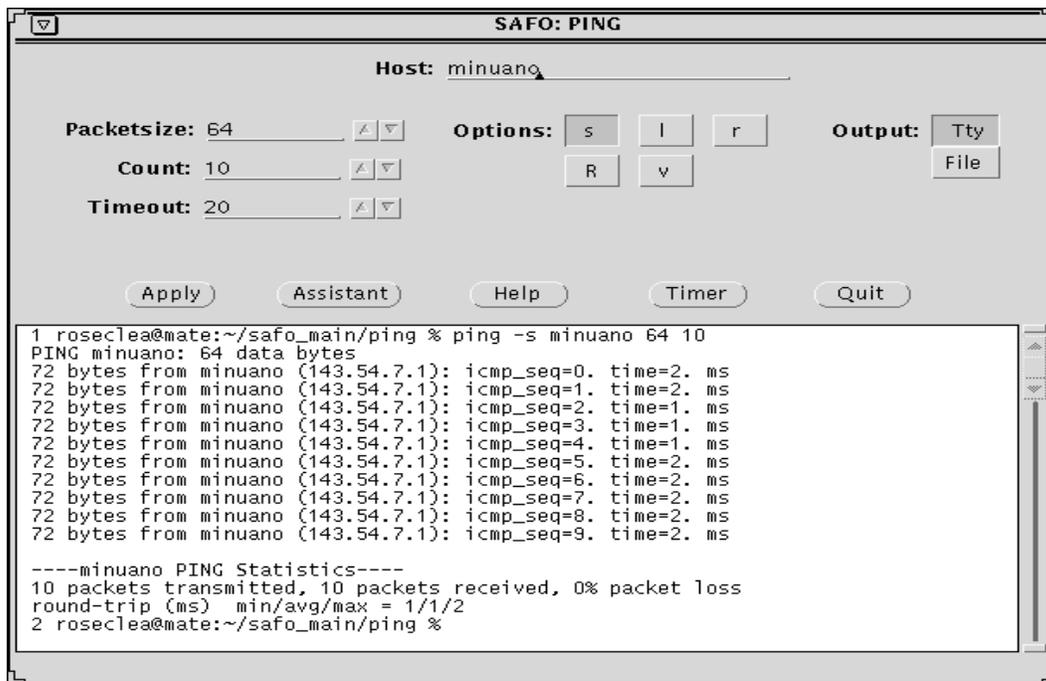


Figura 4: Ping - Interface de Entrada de Parâmetros

Packetsize

Neste campo será informado o tamanho do pacote a ser enviado.

Timeout

Informa o tempo máximo de espera.

Output

O campo 'output' permite que a saída dos resultados seja apresentada na tela (tty), que é a opção default mostrada na figura 4, ou direcione sua saída para um arquivo selecionando a opção 'file'. Neste caso será apresentada uma 'pop-up window' para a entrada de dados, como mostra a figura 5.

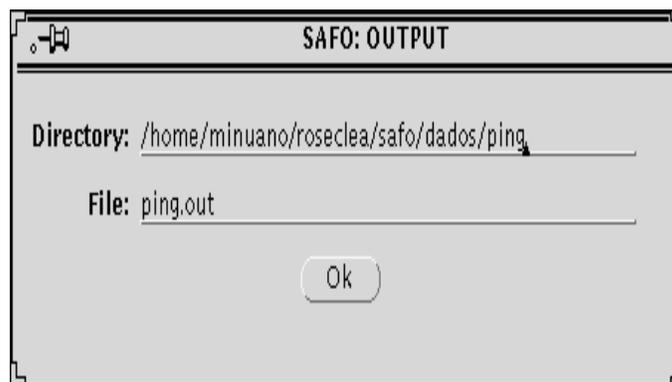


Figura 5: Execução direcionada para arquivo

Nesta janela é solicitado o nome e o diretório do arquivo em que serão gravados os resultados da execução da ferramenta. O armazenamento destas informações será im-

prescindível caso o usuário deseje realizar uma análise sobre as mesmas, pois será este arquivo que servirá de base para as rotinas de tratamento das informações. Cada ferramenta tem seu próprio arquivo de saída.

Timer

Há também a possibilidade de setar no sistema a opção de ‘timer’ de execução das ferramentas, como mostra a figura 6.

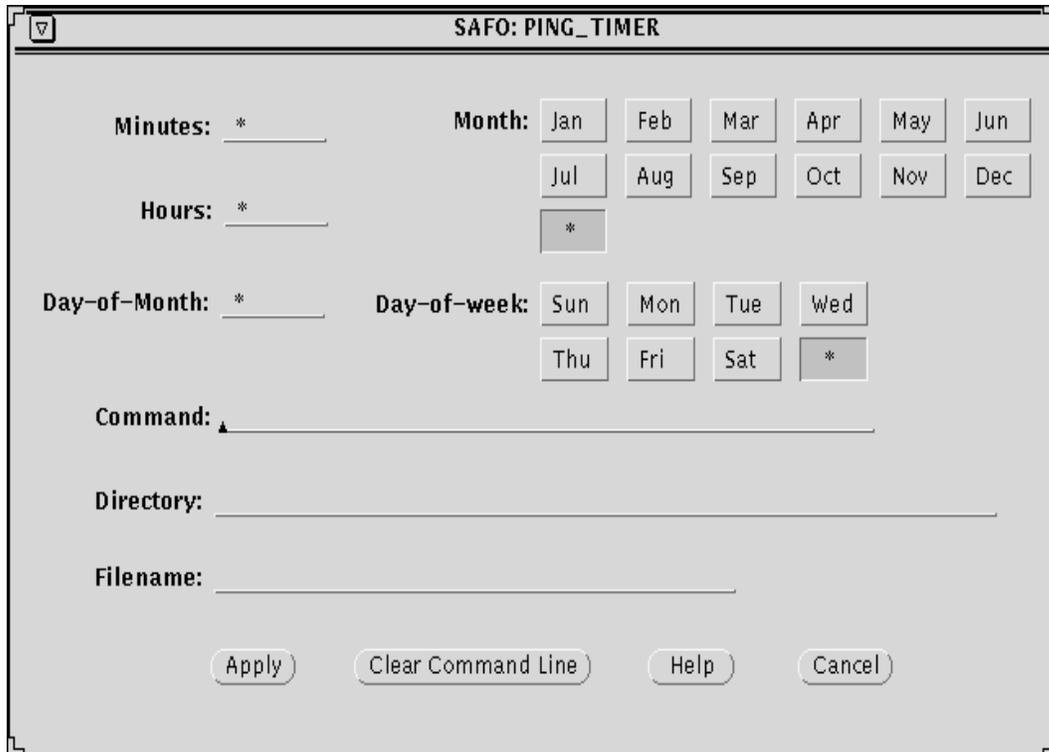


Figura 6: Tempo de execução

Cada ferramenta tem sua opção de ‘timer’. O intervalo de execução (Time interval) pode ser setado para meses, dia da semana, dia do mês e horas/minutos. Nesta janela também é oferecida uma opção de linha de comando. As opções selecionadas são incluídas na ‘cron tab’, permitindo a execução das ferramentas em background. Além de permitir a execução da ferramenta em horários e número de vezes pré-determinados, o ‘timer’ pode ser utilizado em conjunto com a opção ‘output/file’, gerando um arquivo de saída com várias execuções, permitindo assim que seja realizada uma análise de comportamento.

Após o preenchimento dos campos, deve ser pressionado o botão ‘Apply’ para o aceite dos dados e execução da ferramenta.

Inclusão/Exclusão

Para tornar o sistema mais dinâmico, foram implementadas rotinas de inclusão e exclusão de ferramentas. A figura 7 mostra a ‘pop-up window’ apresentada quando é selecionado o botão ‘Inc/Exc’ da janela principal. O Exemplo mostra a inclusão de uma ferramenta chamada ‘prog’.

Nesta ‘pop-up’ é solicitado o preenchimento dos campos ‘label’, que aparecerá na

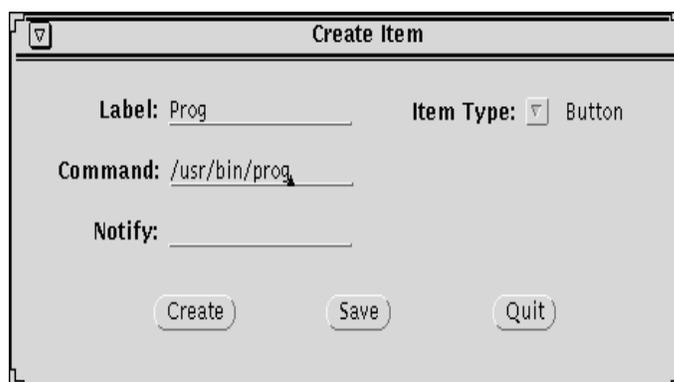


Figura 7: Janela de Inclusão

janela principal juntamente com as demais ferramentas, 'tipo de item', ou seja, se é botão, expressão ou mensagem, e o 'command' que deve ser executado ao ser pressionado o botão da nova ferramenta. Caso esta não esteja no diretório corrente, deve ser informado todo o path. Por último, é solicitada a notificação de execução (opcional).

Ao ser pressionado o botão 'create', o novo label será posicionado na janela principal do SAFO e a ferramenta pode ser executada imediatamente, sem a necessidade de programar/compilar novamente o sistema.

Uma programação adicional somente será necessária no caso de inclusão de ferramenta com parâmetros de execução, os quais o usuário queira disponibilizar em menus. Então será preciso executar a ferramenta de auxílio à criação de interfaces (GUIDE) para criar os botões e seus respectivos menus e compilar novamente todo o sistema. Um exemplo completo para a realização desta tarefa é fornecido com a documentação do sistema.

Exclusão

A exclusão se dá de maneira direta, basta posicionar o cursor sobre a ferramenta e 'arrastá-lo' para fora da janela com o botão 'adjust' do mouse. Esta técnica também é utilizada para re-arranjar o lay-out do sistema.

Tanto a inclusão de novas ferramentas como a exclusão das desnecessárias, torna o sistema mais flexível e direcionado à atender as necessidades específicas do usuário.

Tratamento de Informações e Arquivo de Recomendações

O sistema gera uma grande quantidade de informações de funcionamento, performance, falhas e configuração. Não basta o acúmulo de dados referentes a rede, é necessário saber interpretá-los, processar estas informações para orientar na tomada de decisões. O SAFO proporciona um auxílio para a realização destas tarefas através do botão 'assistant' (figura 8).

Nesta figura temos como exemplo a execução da ferramenta Ping com seu respectivo resultado, no caso a mensagem "unknown host teste". Ao desejar maiores informações sobre aquele resultado o usuário pressiona o botão 'assistant' e lhe é apresentada a tela SAFO:ASSISTANT, com os seguintes campos:

- chave: é a identificação da chave (no exemplo chave 4) que consta do arquivo de recomendações.
- mensagem: é apresentada a mensagem e o nome da ferramenta que gerou.
- prováveis causas da mensagem: o que poderia ter originado aquele tipo de mensagem.

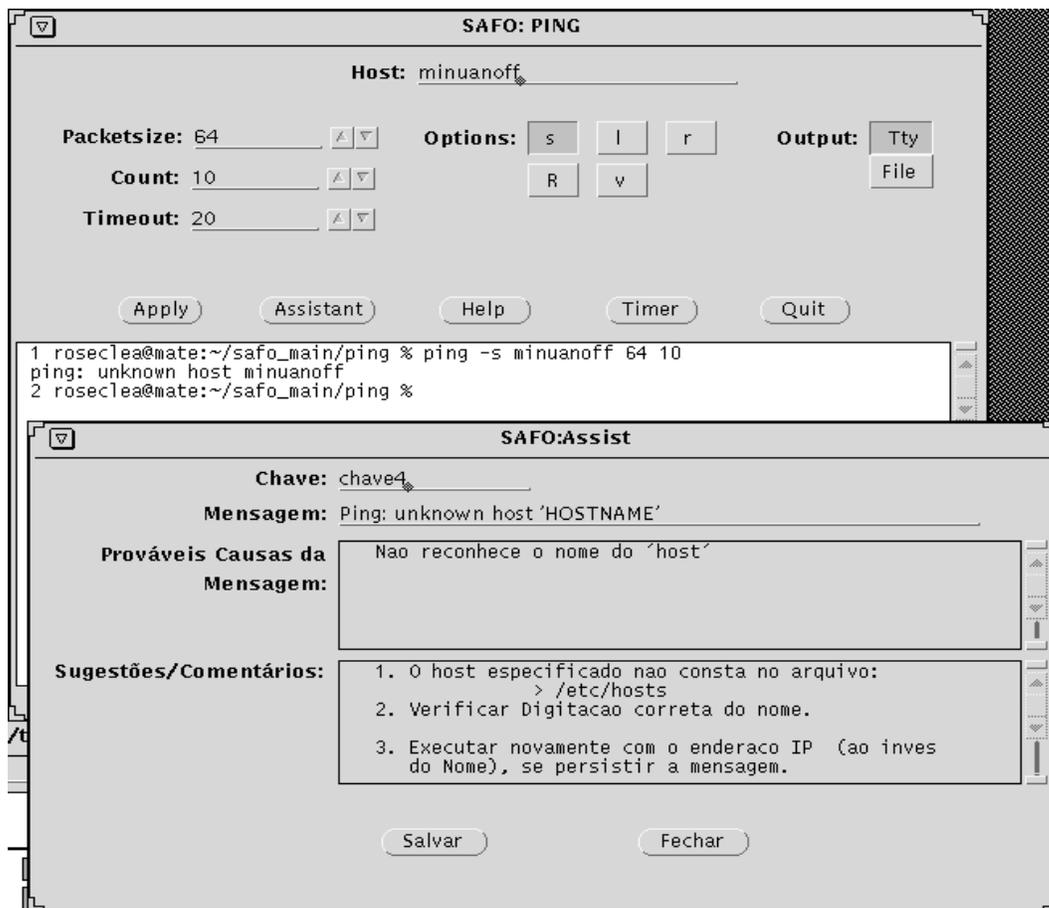


Figura 8: Janela de Tratamento

- sugestões/comentários: sempre que possível, apresenta algumas sugestões para serem executadas e com isso tentar eliminar o problema ou apresenta alguns comentários para facilitar a interpretação da mensagem.

5 Conclusões

Para realização deste trabalho foi necessário um estudo abrangente de várias ferramentas disponíveis principalmente com relação as suas funções e seus mecanismos de funcionamento, com teste extensivo de cada uma pois a documentação sobre elas nem sempre reflete seu estágio real, e alguns parâmetros ou não produzem o resultado esperado ou não produzem resultado algum. Tais observações estão integradas nos sub-menus de help para as ferramentas inicialmente incluídas no SAFO.

O planejamento do sistema usou como fonte o resultado da pesquisa mostrada no item 2, mas, em função dos demais estudos realizados, outras ferramentas estão sendo incluídas.

A utilização do protótipo tem-se apresentado bem mais produtivo do que a modalidade 'command line' usualmente mais utilizada, como visto no início do trabalho. Isto deve-se as várias características práticas do sistema, como ter integradas num único ambiente várias ferramentas de gerenciamento, que podem ser incluídas ou excluídas facilmente conforme as necessidades ou preferências do usuário. O uso dos helps embutidos é mais ágil

e direto do que ‘man page’, além de permitir anotações do próprio usuário. A utilização do ‘timer’ permite uma monitoração constante e pré-determinada da rede e o armazenamento destes resultados num arquivo de saída facilita uma análise posterior.

A implantação das rotinas de tratamento (para auxiliar na interpretação dos resultados das execuções) e das rotinas de interação com um arquivo de recomendações (para auxiliar na tomada de decisões) tornou o sistema ainda mais dinâmico, facilitando o uso das ferramentas, inclusive por operadores inexperientes, e transformando o protótipo do SAFO numa prática e útil ferramenta para simplificar e auxiliar nas funções de gerenciamento.

Referências

- [COM 91] COMER, D. E. **Internetworking with TCP/IP: Principles, Protocols, and Architecture**. Volume 1. Seg. Edição. Prentice-Hall, Englewood Cliffs, NJ, 1991.
- [TAR 90] TAROUCO, LIANE M. R. **Inteligência Artificial Aplicada ao Gerenciamento de Redes de computadores**. *Dissertação de Doutorado*, São Paulo, USP - Escola Politécnica, 1990.
- [STI 90] STINE, R. **FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices** . Request for Comments 1147, 1990.
- [MOC 87] MOCKAPETRIS, P. **Domain Names - Concepts and Facilities** . Request for Comments 1034, 1987.
- [MOC 87] MOCKAPETRIS, P. **Domain Names - Implementation and Specification** . Request for Comments 1035, 1987.
- [SUN 90] Sun Microsystems Inc. **System and Network Administration**. 1990.
- [SUN 90] Sun Microsystems Inc. **SunOS Reference Manual**. Vol I, 1990.
- [SUN 90] Sun Microsystems Inc. **SunOS User's Guide: Getting Started**. 1990.
- [SUN 90] Sun Microsystems Inc. **C Programmer's Guide**. 1990.
- [SUN 90] Sun Microsystems Inc. **Open Windows Developer's Guide 1.1 - User's Manual**. 1990.