
Mali Veith, visipix.com

Ferramentas básicas

Tecendo a Rede

Máquinas em rede oferecem enormes benefícios, mas também significam maior responsabilidade. A partir do momento em que você conecta sua máquina à uma rede, não só se espera que você saiba tudo sobre ela, como também sobre como ela se comunica com o mundo lá fora. Ferramentas comuns podem ajudá-lo a chegar lá... POR NICO LUMMA

Hoje em dia, um computador sem uma conexão com o mundo lá fora parece nos reportar a um mundo pré-histórico.

Embora todas as distribuições Linux atuais instalem os elementos básicos para o funcionamento do computador em uma rede, a responsabilidade por seu gerenciamento ainda fica a cargo dos administradores do sistema – e em alguns casos o treinamento recebido não cobriu como deveria todo o conjunto de técnicas associadas ao funcionamento de uma rede. Neste caso, faz sentido obter o máximo de conhecimento possível sobre o que pode acontecer com computadores ligados em rede.

Os problemas são variados: redes inteiras podem parar de responder, ou uma máquina (como o servidor de internet) pode tornar-se inacessível. Felizmente, a maioria das distribuições Linux já traz todas as ferramentas necessárias para solucioná-los.

Fundamentos de Redes

Infelizmente, a maioria dessas ferramentas assume que você saiba exatamente como uma rede de computadores funciona. O protocolo TCP/IP é o componente básico da Internet e de muitas redes locais. Ele é uma combinação do *Transmission Control Protocol* (Protocolo de Controle de Transmissão - TCP) e do *Internet Protocol* (Protocolo de Internet - IP), e especifica como os computadores devem se comunicar.

Assim como um navegador web não necessita saber se a informação está sendo transmitida via componentes "wireless" ou linhas FDDI e uma linha FDDI não precisa saber se os bits que ela está transportando pertencem a arquivos HTML, MP3s ou vídeos, especialistas usam um modelo de camadas (*layers*) para descrever redes de computadores. Como em uma cebola, cada camada é construída sobre as camadas inferiores, mas, fora isto, cada uma trabalha de forma independente das outras.

A camada de aplicação, como o nome sugere, define como aplicações, tais como navegadores ou programas de email, "conversam" com servidores de Internet ou de email, respectivamente. Como isto ocorre exatamente depende da aplicação. Por exemplo, o Protocolo de Transferência de Hipertexto (HTTP) é utilizado na Internet, enquanto downloads de arquivos normalmente são feitos utilizando o Protocolo de Transferência de Arquivos (FTP).

A camada de transporte reside abaixo da camada de aplicação. Esta camada realiza conexões entre computadores, permitindo que eles troquem dados. O TCP cria uma fila de dados estável entre os pontos de rede (para os protocolos de aplicação HTTP, SSH, POP ou SMTP) e assegura que pacotes perdidos sejam retransmitidos. O outro protocolo mais significativo neste nível é o Protocolo de Datagrama de Usuário (UDP), que pode perder pacotes (e é utilizado, por exemplo, por "streams" do Real Audio).

As coisas começam a ficar realmente interessantes na camada de rede inferior. É nela que os pacotes de dados são colocados na mídia de transporte e tentam encontrar a melhor rota até o seu alvo. Para simplificar esta tarefa, cada pacote inclui os endereços do transmissor e do receptor. Quando uma página da Web é transmitida pelo servidor, os pacotes que a formam podem tomar rotas diferentes. Após aceitar tais pacotes, o receptor deve assegurar que eles serão "remontados" na ordem correta. Além do Internet Protocol (IP), a camada de rede tem protocolos como o *Internet Control Message Protocol* (Protocolo de Controle para

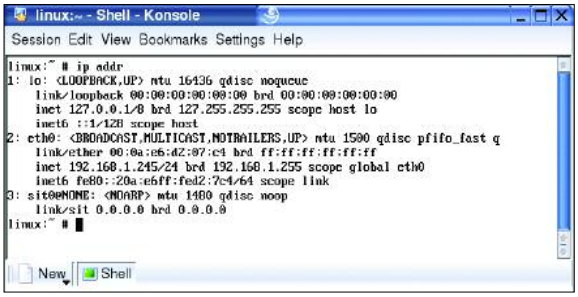

Figura 1: Os dados mostrados pelo comando *ip addr* incluem informações importantes sobre seu endereço de IP. *inet* indica a máscara de rede.

GLOSSÁRIO

DNS: *Servidores DNS possuem bases de dados que são utilizadas para mapear endereços IP a nomes de servidores na Internet (e vice-versa), assim como ocorre em uma lista telefônica. Quando o usuário de uma aplicação de rede tenta acessar um determinado domínio, tais bases de dados são utilizadas pelos servidores DNS para converter o nome digitado no endereço IP do servidor. Assim, quando um usuário digita www.google.com.br, está na verdade acessando o servidor com o endereço IP 216.239.51.104. Será com este endereço que o navegador abrirá uma conexão.*

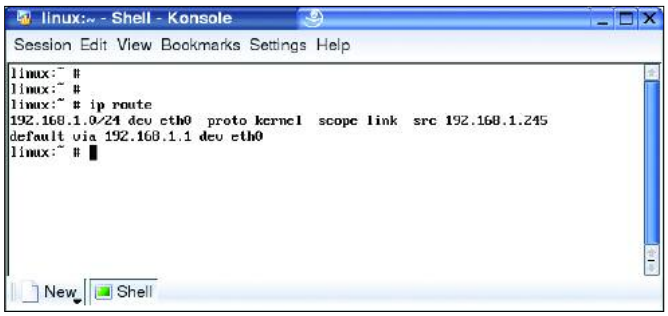

Figura 2: o utilitário *ip route* mostra informações claras a respeito do endereço IP de sua máquina.

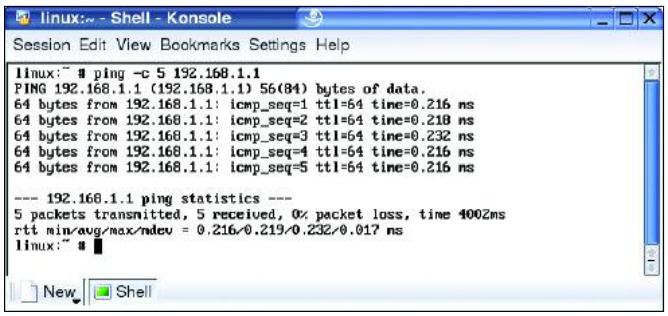

Figura 3: A máquina alvo, que tem o endereço IP 192.168.1.1, respondeu a todos os cinco pings.

Mensagens na Internet - ICMP), para efetuar o controle de mensagens (tais como mensagens de erro), o *Address Resolution Protocol* (Protocolo de Resolução de Endereços - ARP), que associa endereços IP a endereços de hardware (MAC), e seu oposto, o protocolo RARP (*Reverse Address Resolution Protocol* - Protocolo de resolução reversa de endereço).

A camada mais inferior do modelo OSI de camadas é a camada física. Neste nível, a principal preocupação é com a transmissão de bits, bem como a padronização de protocolos para tratar de interfaces elétricas, mecânicas e de sinalização. Isto inclui padrões como o RS-232 e X.21.

Os componentes de uma rede são identificados através dos seus endereços IP. O TCP pode retransmitir pacotes perdidos ou danificados, assegurando que o receptor contará com, pelo menos, um conjunto completo dos pacotes enviados. Os protocolos de aplicação, por mais sofisticados que sejam, se baseiam neste serviço. Sem um pouco de conhecimento sobre as camadas citadas acima, muitas ferramentas de rede não farão nenhum sentido.

Verificação de Status

Antes de começar a analisar o tráfico de dados na rede, é importante certificar-se de que seu computador está realmente utilizando a rede como deveria.

Para encurtar a história, cada máquina necessita um endereço IP (também conhecido como *IP Address*) único para ser capaz de comunicar-se com as outras máquinas da rede. Um *gateway* permite que pacotes de dados com destino à Internet possam deixar a rede local.

O comando *ip* fornece detalhes sobre a sua configuração atual. Sistemas mais antigos talvez tenham somente os comandos *ifconfig* e *route*, que mostram a mesma informação, embora de forma ligeiramente diferente. Se o seu shell não é capaz de encontrar nenhum destes comandos, pode ser que eles tenham sido instalados no diretório */sbin*, que não está normalmente no *search path* (rota de busca) do sistema. Neste caso, basta informar o caminho inteiro quando quiser rodar o programa (ex: */sbin/ip*).

A opção *addr* indica ao comando *ip* que ele deve fornecer dados sobre a placa de rede. A linha finalizada por *eth0* indica a primeira placa de rede do sistema (*eth1* é a segunda – possivelmente utilizada para WLAN, e assim por diante). Ela mostra o endereço IP do computador (192.168.1.245 na Figura 1), a máscara de rede (/24), o endereço de broadcast (192.168.1.255) e o nome da interface de rede (eth0).

O resultado do comando *ip route* é mais fácil de ler (ver Figura 2). A primeira linha mostra a rede (o endereço da rede no nosso exemplo é 192.168.1.0) e a netmask (/24), a interface de rede e, por fim, a chamada *data source* (por isso o termo *src*, indicando "source") que é o endereço IP (192.168.1.245). A segunda linha indica o *default gateway*, cujo endereço IP é 192.168.1.1.

Caso informações importantes, tais como os endereços IP da máquina e do

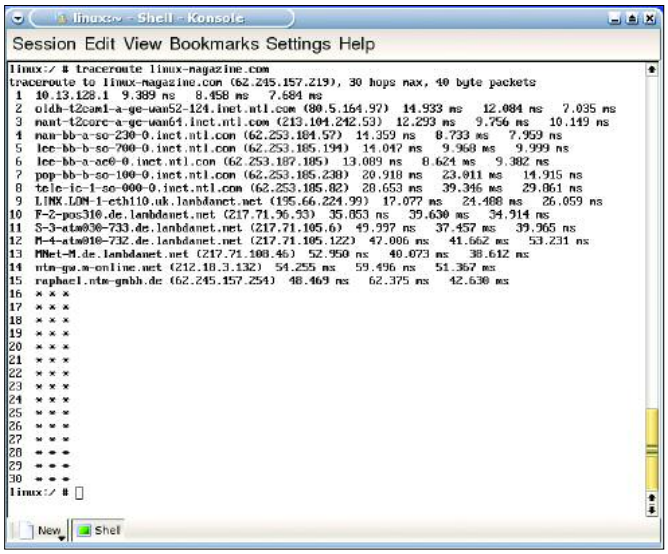

Figura 4: *traceroute* mostrando a rota para "www.linuxmagazine.com.br".

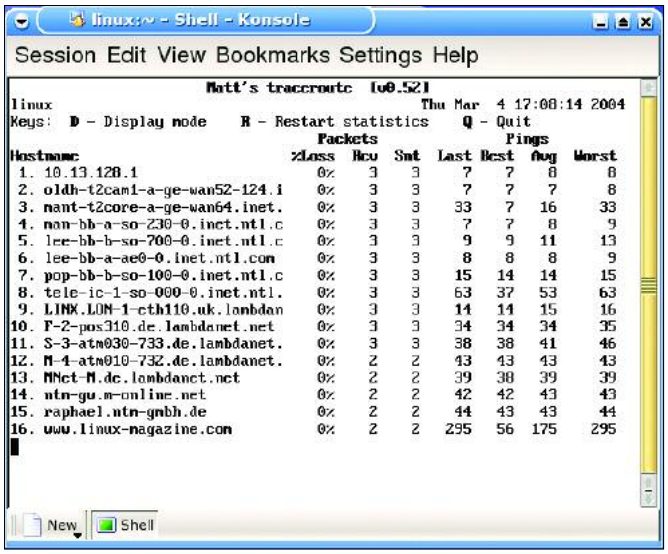

Figura 5: o *mtr* combina os resultados de *traceroute* e *ping*.

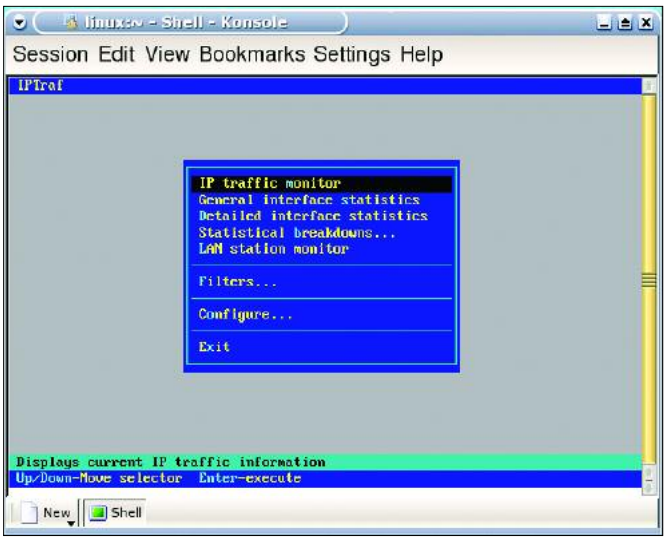

Figura 6: *iptraf* é útil, mesmo sem uma configuração e filtro exclusivos.

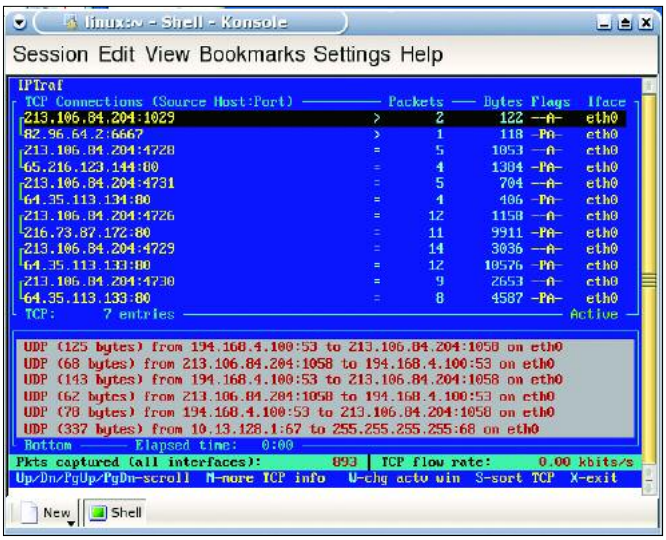

Figura 7: Quantos pacotes estão indo e vindo para qual endereço?

gateway, estiverem faltando aqui, isto pode explicar porque o seu computador não está se comportando como deveria na rede. Neste caso, rode a ferramenta de configuração da sua distribuição (como o YaST, no caso do SuSE Linux), verifique a configuração de rede do seu sistema e tente novamente.

Ping-Pong

ping é uma ferramenta simples para análise da rede, mas é também extremamente prática. Ela transmite pacotes de dados ICMP do seu computador para um computador alvo e mostra o tempo que cada resposta leva para retornar ao seu computador – assumindo que o computador alvo responda. A seção final do resultado de um ping é um grupo de estatísticas que mostram a você quantos pacotes foram transmitidos (cinco na Figura 3), quantas respostas retornaram (cinco novamente) e quanto tempo isto levou para acontecer (4002 milisegundos). Se pacotes fossem descartados ou perdidos, tais estatísticas os mostrariam em uma seção chamada *packet loss*. Se o computador alvo não está acessível, nada acontece por um tempo, enquanto o ping aguarda por respostas.

O comando *ping hostname* transmite pacotes ICMP sem parar até que você pressione [Ctrl-C]. Você também pode especificar *ping -c 10 hostname* para transmitir apenas dez pacotes.

Rotas

Enquanto ping só mostra se o computador alvo está respondendo, *traceroute* mostra todo o caminho que os pacotes de dados tomaram até atingi-lo (ver Figura 4). Os asteriscos (*) indicam que um erro ocorreu no roteamento, ou que um firewall bloqueou a passagem deste tipo de pacote de dados. Aliás, a opção *-n* pode ser utilizada para evitar que os hostnames sejam mostrados. Para indicar qual a interface de rede a ser usada, utilize a opção *-i*.

O comando *mtr targethost* mostra a rota dos pacotes de forma mais clara (ver Figura 5), pois indica exatamente onde os pacotes estão tendo atrasos maiores (caso você não pressione a tecla [q]). Para cada trecho da rota, *mtr* descobre o que está acontecendo com os pacotes de dados. Por isso, mtr pode ser visto como uma combinação entre ping e traceroute. Por exemplo, o comando:

```
mtr -c 10 --report ➥
targethost
```

informa ao mtr para transmitir apenas dez pacotes, parar e fornecer um relatório. A coluna *HOST* indica onde o pacote de dados se encontra, *LOSS* informa a porcentagem de pacotes descartados ou perdidos, *RCVD* e *SENT* mostram, respectivamente, quantos pacotes foram recebidos e enviados e as colunas *BEST*, *WORST* e *AVG* informam quanto tempo a transmissão dos pacotes levou, no melhor e no pior dos casos, e também na média.

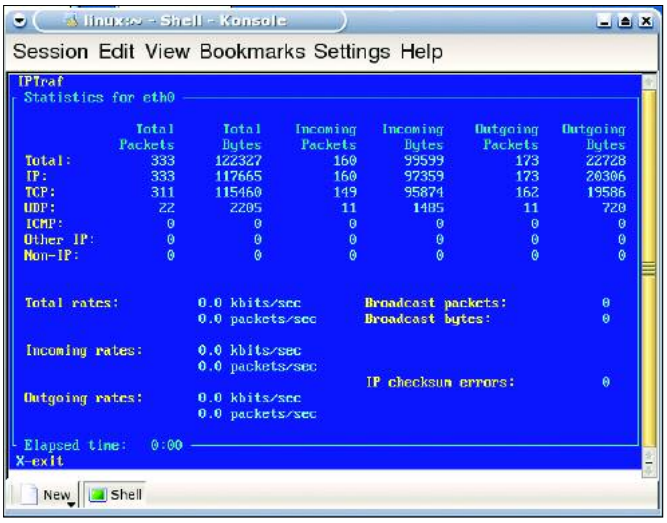

Figura 8: *iptraf* fornece estatísticas detalhadas sobre a rede.

Para obter maior precisão...

... experimente usar *tcpdump*, a ferramenta de análise de rede de mil e uma utilidades. A maioria das distribuições Linux já fornece um pacote de instalação. Caso contrário, o código fonte pode ser baixado em [1]. Se quiser compilar seu próprio binário, você vai precisar da biblioteca *libcap*.

O tcpdump precisa de privilégios de administrador para rodar, uma vez que ele coloca a placa de rede em modo "promíscuo", o que permite a ela ler

quaisquer pacotes que passem pela interface de rede local, inclusive a captura de dados.

O tcpdump mostra todos os pacotes de dados que aparecem na interface da placa de rede:

```
11:56:27.833598 192.168.1.245 ➥
.ssh > 192.168.1.20.39258: P ➥
1392512:1392720(208) ack 1201 ➥
win 9120 <nop,nop,timestamp ➥
2599771999 1711932971> (DF) ➥
[tos 0x10]
```

Em nosso exemplo pode ser visto que a máquina com o IP 192.168.1.245 enviou um pacote de dados ssh para a máquina com o IP 192.168.1.20. Digite:

SOBRE O AUTOR

Nico Lumma é o Diretor de TI da Orangemedia.de GmbH, empresa especializada na comercialização de espaço publicitário online, e conta com anos de experiência no uso do Linux em ambientes empresariais.

```
tcpdump -i eth0 port 80
```

e os dados destinados à porta TCP número 80 – comumente utilizada por servidores de Internet – serão mostrados. Por outro lado, *tcpdump host targethost* fornecerá o tráfico de rede em targethost.

Pra onde?

É importante instalar ferramentas especializadas de modo a não ficar "no escuro" no que concerne à utilização da rede. O *iptraf* é um exemplo. Ele mostra exatamente o que está acontecendo com a placa de rede, que protocolos estão sendo utilizados atualmente e com que outras máquinas a máquina sob análise está "conversando". Pressione as teclas [q] e [Enter] para encerrar o programa.

No menu principal (ver Figura 6) há um item chamado *IP Traffic Monitor* (ver Figura 7), que fornece uma visão geral do tráfego dos dados na rede, e permite a identificação de pontos de sobrecarga.

Por outro lado, o item *Detailed Interface Statistics* (ver Figura 8) não indica quais máquinas estão trocando dados, mas analisa o fluxo do tráfego, classificado por protocolo. Isto fornece informações úteis sobre a taxa transferência de dados e indica onde se encontram problemas de performance (os chamados gargalos ou *bottlenecks*). Por exemplo, se há mais saída do que entrada de dados, pode-se assumir que alguém está baixando algo do seu micro.

Teríamos muito mais a relatar sobre *iptraf* e outras ferramentas mencionadas neste artigo. Se o leitor quer melhorar seus conhecimentos nesta área, não há alternativa: adquira o máximo de conhecimento e experiência possível. ■

INFORMAÇÕES

[1] Tcpdump: *http://www.tcpdump.org*

[2] IPTraf: *http://cebu.mozcom.com/riker/iptraf*

[3] Conjunto de protocolos da Internet: *http://en.wikipedia.org/wiki/TCP/IP*

[4] Protocolo TCP: *http://en.wikipedia.org/wiki/Transmission_Control_Protocol*

[5] Protocolo IP: *http://en.wikipedia.org/wiki/Internet_Protocol*