Capítulo 3:COMANDOS EM REDES TCP/IP

3.1 Comandos básicos

3.1.1 ping

Com certeza, o ping (Packet INternet Groper) é o comando mais difundido para o teste de redes. Com ele poderemos saber se um pacote está chegando no seu destino ou não. Basta utilizar o nome ou endereço IP do host de destino para testar. Exemplos:

Comando	Resultado
# ping 10.0.0.1	Verifica se há conexão com a máquina 10.0.0.1.
# ping micro1.rede.com.br	Verifica se há conexão com a máquina micro1.rede.com.br.

3.1.2 arp

Além do endereço IP atribuído a cada adaptador de rede, este já vem de fábrica com um outro tipo de endereço fixo chamado endereço MAC. O endereço MAC é constituído por 06 valores hexadecimais, entre 00h e FFh, separados por dois pontos. Exemplos:

02:60:8C:3E:B3:23

08:00:5A:5C:55:55

Os três primeiros números identificam o fabricante e os três últimos o adaptador de rede. Por exemplo: 08:00:5A representa a IBM. No mundo inteiro, teoricamente, não existem duas placas de rede com o mesmo endereço MAC original de fábrica. No entanto, o endereço MAC pode ser modificado pelo usuário.

A distribuição dos ranges de endereços MAC é determinado pelo pelo IEEE. A relação oficial encontra-se em http://standards.ieee.org/regauth/oui/oui.txt .

Chaves mais importantes:

Chave	Função
-n	Força o arp a não resolver nomes, acelerando os tempos de resposta.
-a	Mostra todos os endereços MAC de máquinas que, recentemente, mantiveram algum tráfego com máquina local.

Como o endereço MAC está implementado na camada 2 da pilha TCP/IP, só serão mostrados os MAC da rede local. Caso haja roteamento para chegar a uma determinada máquina, será mostrado o MAC do adaptador de rede do roteador. Ainda, geralmente, a opção -n é utilizada com comandos em redes para evitar a resolução de nomes.

3.1.3 arping

Instale com: # apt-get install arping

Uma mistura de ping e arp. Retorna o endereço MAC do adaptador remoto que está sendo "pingado". Exemplo:

arping 10.0.0.1

Obs: não irá pingar máquinas que não pertençam à rede local.

3.1.4 ifconfig

O comando ifconfig mostra as configurações de todos os adaptadores de rede existentes na máquina. Também pode ser utilizado para configurar adaptadores de rede. Exemplos:

Comando	Resultado
# ifconfig eth0 down	Retira o adaptador eth0 do ar.
# ifconfig eth0 10.0.0.1 netmask 255.0.0.0	Coloca no ar o adaptador eth0 com o endereço IP e a máscara de rede citados. Também pode ser utilizado para alterar o endereço IP ou a máscara de rede de um adaptador que já esteja em funcionamento.

Cabe ressaltar que os dados inseridos com o ifconfig serão perdidos caso o a rede ou o host sejam reiniciados.

Caso necessite configurar o default gateway, utilize o comando route. Um exemplo:

Comando	Resultado
# route add -net default gw 10.1.1.1	Determina que o default gateway para este host será a máquina 10.1.1.1.

3.1.5 netstat

Este comando fornece dados diversos sobre a rede.

Chave	Função
-n	Força o netstat a não resolver nomes, acelerando os tempos de resposta.
-i	Fornece uma relação de interfaces de rede e dados como MTU, dados trafegados etc.
-r	Mostra a tabela de roteamento.
-l	Mostra somente as portas referentes aos serviços que estejam ativos.
-a	Mostra todas as conexões ativas e as portas abertas (clientes e servidoras).
-s	Mostra estatísticas por protocolo.
-t	Mostra somente as conexões TCP.
-u	Mostra somente as conexões UDP.
-p	Mostra os processos que estão abrindo as portas ativas.
-c	Atualiza os dados na tela a cada segundo.

Exemplos:

Comando	Resultado
# netstat -tunap	Mostra todas as conexões e portas TCP e UDP ativas (clientes e servidoras), sem resolver nomes, e citando os nomes dos processos que estão abrindo tais portas.
# netstat -tuap	Idem ao anterior, resolvendo nomes. Isso poderá ser demorado.
# netstat -tnl	Mostra somente as portas TCP servidoras abertas, sem resolver nomes.
# netstat -unl	Mostra somente as portas UDP servidoras abertas, sem resolver nomes.
# netstat -tunlp	Mostra portas TCP e UDP servidoras abertas, sem resolver nomes, e quais processos estão ativando tais portas. Ideal para a verificação de segurança.

3.1.6 dhclient

Busca as configurações de rede em um servidor dhcp. Em outras distribuições poderão existir outros comandos similares, como dhcpcd e pump (Knoppix, por exemplo). Também é possível determinar qual interface deverá buscar por um servidor dhcp. Exemplo:

```
# dhclient eth1
```

3.2 Comandos para acesso a serviços remotos

3.2.1 telnet

O telnet permite controlar remotamente outra máquina (servidora telnet). Em conseqüência, o daemon telnetd deverá estar habilitado na máquina de destino.

Para acessar a outra máquina, digite:

```
# telnet <nome do servidor>
```

ou

```
# telnet <IP do servidor>.
```

Depois disso você deverá entrar com o nome e senha de um usuário cadastrado. Por segurança, o sistema não aceitará o usuário root.

Principais opções dentro do ambiente:

Opção	Função
Ctrl]	Desfaz a conexão, permanecendo no ambiente telnet.
quit	Abandona o ambiente telnet.
su -	Permite tornar-se root, depois de conectado.

Podemos ainda executar um telnet direto para uma porta TCP de um servidor para testar o seu status. Exemplos:

Comando	Resultado
# telnet 10.0.0.1	Executa telnet no server 10.0.0.1.
# telnet 10.0.0.1 25	Executa telnet na porta 25 TCP do host 10.0.0.1.

Os dados de telnet trafegam em claro, inclusive as senhas. Sempre que possível, utilize ssh, ao invés de telnet.

O cliente telnet do Windows não é dos melhores. Sugiro utilizar o programa PuTTy, disponível em http://www.chiark.greenend.org.uk/~sgtatham/putty.

O servidor telnet poderá ser instalado no Debian com o comando # apt-get install telnetd.

3.2.2 ssh

Instale com: # apt-get install ssh. Ao instalar o cliente ssh, também será instalado o servidor ssh.

Esse é o modo mais seguro e atual se fazer o controle remoto de máquinas. Similar ao telnet, com a diferença de que os dados trafegam criptografados.

Para que possamos executar o ssh em direção a uma máquina, o seu daemon ssh deverá estar rodando. Exemplos:

Comando	Resultado
# ssh 10.0.0.1	Executa ssh no servidor 10.0.0.1 como root, uma vez que o usuário logado é o root e não foi especificado um usuário diferente com a sintaxe usuário@host_destino.
# ssh eriberto@10.0.0.1	Executa ssh no servidor 10.0.0.1 como eriberto.

Obs: o PuTTy é o melhor cliente ssh para Windows.

No primeiro login será mostrado o fingerprint da máquina servidora. O fingerprint é uma cadeia de bytes aleatórios, gerados durante a instalação do servidor. Caso outra máquina com o mesmo IP tente se passar pelo servidor, o cliente será avisado. Neste caso, para realizar a conexão, será necessário remover o fingerprint referente ao IP da máquina da tabela de hosts conhecidos existente no cliente. A tabela de hosts conhecidos é o arquivo /home/user/.ssh/known_hosts, onde /home/user é o diretório home do usuário (poderá ser somente /root).

O comando ssh possui algumas chaves interessantes:

Chave	Função
-X	Permite a execução remota de aplicativos gráficos.
-C	Faz a compressão dos dados a serem enviados.
-p	Permite designar a porta de login para um determinado servidor.

3.2.3 ftp

Instale com: # apt-get install ftp

File Transfer Protocol ou Protocolo de Transferência de Arquivos. Utilizado para fazer download/upload de arquivos remotamente, a partir de servidores FTP (que estarão com o daemon ftp no ar). Para executar, digite ftp <nome do servidor> ou ftp <IP do servidor>. Depois disso você deverá entrar com o nome e senha de um usuário cadastrado. As principais opções dentro do ambiente são:

Opção	Função
bye	Abandona a sessão e o ambiente ftp.
by	O mesmo que bye.
close	Abandona a sessão ftp.
?	Tela de comandos disponíveis.
? <comando>	Ajuda do comando.
asc	Define o download/upload em modo ASC II.
bin	Define o download/upload em modo binário.
bell	Emite bip quando um comando é completado.
cd	Muda o diretório remoto.
lcd	Muda o diretório local ou mostra o atual.
delete	Deleta o arquivo remoto.
get	Faz download. Não aceita curingas (* e ?).
put	Faz upload. Não aceita curingas (* e ?).
mget	Faz download. Aceita curingas (* e ?).
mput	Faz upload. Aceita curingas (* e ?).

prompt off	Desabilita o modo interativo.
prompt on	Habilita o modo interativo.
ls	Lista conteúdo do diretório remoto.
mdelete	Deleta arquivos remotos. Aceita curingas.
mkdir	Cria diretório na máquina remota.
pwd	Mostra o diretório remoto corrente.
rename	Renomeia arquivo no diretório remoto.
rmdir	Remove diretórios vazios na máquina remota.
status	Mostra status da sessão.
user	Conecta um novo usuário. Útil depois de close.

Com o ftp, poderemos realizar operações de upload (caminho cliente-servidor) e download (caminho servidor-cliente). O MODO DE OPERAÇÃO MAIS CONFIÁVEL E EFICIENTE É O BINÁRIO, pois se aplica a qualquer tipo de arquivo. O modo ASC II só pode ser utilizado com arquivos em formato texto plano.

Muitos servidores ftp estão disponíveis para login anônimo. Em servidores anônimos o login deverá ser "anonymous". A senha a ser inserida será o e-mail do usuário.

O melhor servidor ftp para Linux é o Proftpd e poderá ser instalado com o comando # apt-get install proftpd.

3.2.4 scp

O scp faz parte do pacote ssh.

Uma mistura de cp, ftp e ssh. Faz transferência de arquivos, de forma criptografada, entre hosts. Exemplos:

Comando	Resultado
# scp teste.sh root@10.0.0.1:/etc/adm	Irá logar como root na máquina 10.0.0.1, transferir o arquivo teste.sh para o diretório /etc/adm para o diretório da máquina 10.0.0.1.
# scp root@10.0.0.1:/etc/adm/teste.sh .	Nesse caso, será feito login na máquina 10.0.0.1, como root, e haverá uma transferência do arquivo /etc/adm/teste.sh para o diretório local (sentido 10.0.0.1 - máquina local).

3.3 Comandos para consulta de domínios

3.3.1 nslookup

Instale com: # apt-get install dnsutils

Name server lookup. Realiza pesquisas em servidores DNS. Extremamente útil para a verificação de funcionamento de servidores DNS e para o levantamento de dados sobre domínios e endereços. Exemplos:

Comando	Resultado
# nslookup 10.20.2.5	Busca pelo nome referente ao endereço IP informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.

# nslookup www.uol.com.br	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.
# nslookup www.uol.com.br 200.176.2.172	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o 200.176.2.172.
# nslookup www.uol.com.br ns1.terra.com.br	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o ns1.terra.com.br.

3.3.2 dig

Instale com: # apt-get install dnsutils

Assim como nslookup, faz pesquisas em servidores DNS. Para verificar endereços IP, utilizar a chave -x. Exemplos:

Comando	Resultado
# dig -x 10.20.2.5	Busca pelo nome referente ao endereço IP informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.
# dig www.uol.com.br	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.
# dig www.uol.com.br @200.176.2.172	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o 200.176.2.172.
# dig www.uol.com.br @ns1.terra.com.br	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o ns1.terra.com.br.
# dig uol.com.br	Mostra dados gerais sobre o domínio informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.
# dig mx uol.com.br	Mostra quem são os servidores MX (SMTP) do domínio informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf. Outro servidor DNS poderá ser informado com @.
# dig ns uol.com.br	Mostra quem são os servidores NS (DNS) do domínio informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf. Outro servidor DNS poderá ser informado com @.
# dig uol.com.br	Mostra quem é o administrador e outros dados do domínio informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf. Outro servidor DNS poderá ser informado com @.

3.3.3 host

Instale com: # apt-get install host

Possui as mesmas funções do nslookup e fornece resultados semelhantes. Com a opção -l, tenta fazer download da relação completa de hosts listados no servidor. Isso só será possível se o servidor DNS estiver permitindo a transferência de zona. Ideal para teste de segurança. Exemplos:

Comando	Resultado
# host 10.20.2.5	Busca pelo nome referente ao endereço IP informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.
# host www.uol.com.br	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o existente em /etc/resolv.conf.
# host www.uol.com.br 200.176.2.172	Busca pelo endereço IP referente ao nome informado. O servidor DNS ser utilizado será o 200.176.2.172.
# host -l dominio.com.br	Tenta fazer download da relação completa de hosts listados no servidor (atuação como DNS secundário). Esta opção pode ser utilizada como teste da segurança.

3.3.4 whois

Instale com: # apt-get install whois

Mostra os dados completos de domínios e blocos IP na Internet. Exemplos:

Comando	Resultado
# whois uol.com.br	Mostra dados sobre o domínio uol.com.br.
# whois 200.252.148.144	Mostra dados sobre o bloco ao qual o endereço IP em questão pertence.

3.3.5 geoip

Instale com: # apt-get install geoip-bin

Mostra a localização de um endereço IP ou máquina pelo nome. Exemplos:

Comando	Resultado
# geoiplookup www.uol.com.br	Mostra dados sobre o domínio uol.com.br.
# geoiplookup 200.252.148.144	Mostra dados sobre o bloco ao qual o endereço IP em questão pertence.

3.4 Comandos para o rastreamento de rotas

3.4.1 traceroute

Instale com: # apt-get install traceroute

Mostra a rota que os pacotes percorrerão entre o host origem e o host destino. Utiliza pacotes UDP por default. Com -I usará pacotes ICMP. Exemplos:

Comando	Resultado
# traceroute 10.40.55.12	Mostra a rota percorrida entre a origem e o host 10.40.55.12, utilizando o protocolo UDP.
# traceroute -I www.uol.com.br	Mostra a rota percorrida entre a origem e o host www.uol.com.br, utilizando o protocolo ICMP.
# traceroute -p 53 ns1.terra.com.br	Mostra a rota percorrida entre a origem e o host www.uol.com.br. Utiliza a porta 53 UDP como destino (o default é 33434).

3.4.2 tcptraceroute

Instale com: # apt-get install tcptraceroute

Similar ao traceroute. É utilizado para ultrapassar bloqueios em firewalls, pois utiliza TCP, ao invés de UDP e ICMP.

3.4.3 mtr

Instale com: # apt-get install mtr

O MRT é uma ferramenta que mostra, de forma interativa e constantemente atualizada, as rotas utilizadas para interligar dois pontos na Internet. Para executar, utilize o comando # mtr <endereço>. A tecla h oferece algumas opções.

3.5 Comandos para o navegação e download em shell

3.5.1 lynx

Instale com: # apt-get install lynx

Utilizado para navegação http em modo texto. Com -dump retorna ao prompt após exibir o conteúdo da URL. Exemplos:

Comando	Resultado
# lynx www.google.com.br	Acessa o site www.google.com.br.
# lynx -dump www.google.com.br	Acessa o site wwww.google.com.br, mostrando a página principal, e retorna imediatamente para o prompt.

lynx: um dia você ainda vai precisar dele!

3.5.2 elinks

Instale com: # apt-get install elinks

Utilizado para navegação http em modo texto. Um pouco mais avançado do que o lynx e com suporte a frames.

3.5.3 wget

Utilizado para fazer download de arquivos e diretórios em modo texto. Suporta os protocolos http e ftp. Sintaxe:

wget <endereço web ou ftp>

Principais chaves:

Chave	Função
-c	Continua o download a partir do ponto no qual o mesmo foi interrompido.
-r	Faz download recursivo.
-l	Estabelece o nível máximo de diretórios que serão copiados com -r. O default é 5.
-t0	Tenta quantas vezes for necessário estabelecer a conexão. O valor default é 20. Erros críticos como “404 not found” irão cancelar definitivamente as tentativa.

-nc	Não faz download de arquivos que já tenham sido baixados.
--retr-symlinks	Segue os links existentes.
-m	Faz um mirror local. Não pode ser utilizado em conjunto com outras opções. É recursivo e não baixa arquivos que já tenham sido baixados.

Exemplo:

```
# wget http://cdimage.debian.org/debian-cd/3.1_r2/i386/iso-cd/debian-31r2-i386-netinst.iso
```

3.6 Comandos de vasculhamento e análises em redes

3.6.1 nmap

```
Instale com: # apt-get install nmap
```

Permite o vasculhamento de redes, de forma a buscar hosts ativos, portas abertas etc. Exemplos de utilização:

Comando	Resultado
# nmap <host>	Mostra todas as portas abertas no host.
# nmap 10.0.0.*	Mostra todas as portas abertas nos hosts existentes dentro da faixa IP 10.0.0.1 a 10.0.0.254.
# nmap -sP 10.0.0.2-50	Executa um ping, por host, no intervalo de 10.0.0.2 a 10.0.0.50.
# nmap -p 137-139 10.0.0.*	Procura pela existência das portas 137 a 139 nos hosts que possuam IP iniciado por 10.0.0.
# nmap -p 25,80 10.*.*.1	Procura pela existência das portas 25 e 80 nos hosts que possuam IP com 10 no primeiro octeto e 1 no último.
# nmap -O <host>	Busca por todas as portas abertas, utilizando o sistema de fingerprint para tentar descobrir o sistema operacional do host.
# nmap -sU -p 53 10.0.20-50.*	Procura pela existência da porta 53 UDP nos hosts de 10.0.20.0 a 10.0.50.255.
# nmap <ação> 10.0.0.0/8	Executa uma ação em toda a rede 10.0.0.0 (máscara classe A).

3.6.2 iptraf

```
Instale com: # apt-get install iptraf
```

Fornece dados referentes ao tráfego de rede como conexões ativas, portas em uso, velocidade do fluxo de dados nos adaptadores de rede etc.Permite o uso de filtros e pode funcionar em modo promiscuous.

3.6.3 sniffit

```
Instale com: # apt-get install sniffit
```

O sniffit é um analisador de tráfego que pode fornecer importantes dados sobre a rede, ajudando a descobrir problemas diversos.

Para analisar conexões TCP, é melhor rodá-lo no modo interativo. Para isso, execute:

```
# sniffit -I
```

3.6.4 tcpdump

```
Instale com # apt-get install tcpdump
```

O tcpdump é o melhor analisador de tráfego em modo texto que existe. Mostra as conexões estabelecidas e o tráfego correspondente. As chaves mais importantes são as seguintes:

Chave	Função
-A	Mostra também o conteúdo dos pacotes utilizando caracteres ASCII.
-X	Mostra também o conteúdo dos pacotes utilizando seqüências em hexadecimal e caracteres ASCII.
-s tamanho	Permite especificar a quantidade de bytes que será capturada por pacote. O valor default é 96. Para capturar o conteúdo total em redes ethernet, deverá ser especificado o valor 1500. Esta opção só terá sentido se utilizada com -X.
-v	Aumenta a quantidade de informações extraídas do cabeçalho do pacote.
-vv	Idem ao anterior, com mais informações ainda.
-vvv	Idem ao anterior, com mais informações.
-w arquivo	Grava o resultado em um arquivo.
-r arquivo	Lê um arquivo previamente gravado com -w.
-t	Não mostra a data e a hora.
-tttt	Mostra a data e a hora utilizando o padrão "yyy-mm-dd hh:mm:ss.ssssss", em formato UTC.
-n	Não faz resolução reversa de nomes de hosts, acelerando a aparição dos resultados (tempo real).
-N	Se fizer resolução de nomes, não mostra o domínio do host.
-i interface	Analisa somente os dados que passarem pela interface de rede especificada. A interface padrão é a primeira listada pelo comando ifconfig. O valor “any” poderá ser utilizado para capturar dados em todas as interfaces. No entanto, “any”não funciona em modo promiscuous.
-p	Não utiliza o modo promiscuous.
-S	Mostra os resultados ordenados pela seqüência absoluta do TCP.

Além das chaves, o tcpdump admite expressões de filtragem. As expressões mais utilizadas com o tcpdump são as seguintes:

Expressão	Significado
dst host <nome/ip>	Refere-se ao host de destino declarado pelo seu nome ou endereço IP.
src host <nome/ip>	Idem, referindo-se ao host de origem.
host <nome/ip>	Idem, referindo-se ao host, sem distinguir se é de origem ou destino.
dst net <rede/CIDR>	Refere-se a uma rede de destino declarada pelo fragmento do endereço IP comum para toda a rede. Ex: 172.20.
src net <rede/CIDR>	Idem, referindo-se a uma rede de origem.
net <rede/CIDR>	Idem, referindo-se à rede, sem distinguir se é de origem ou destino.
dst port <porta>	Refere-se a uma porta de destino, declarada pelo seu número. Em caso de dúvidas, consultar o arquivo /etc/services.
src port <porta>	Idem, referindo-se a uma porta de origem.
port <porta>	Idem, referindo-se à porta, sem distinguir se é de origem ou destino.
ether host <mac>	Refere-se a um endereço MAC, sem distinguir se é de origem ou destino.
<ip proto>	Refere-se a um protocolo IP. Em caso de dúvidas, consultar o arquivo /etc/protocols. Em algumas poucas circunstâncias será necessário usar “ip proto <protocolo>”. Ex: ip proto ospf. Nas demais circunstâncias, os protocolos poderão ser citados diretamente. Ex: tcpdump icmp -n.
not ou !	Operador lógico NOT. Utilizado para excluir algo do resultado da pesquisa.

and ou &&	Operador lógico AND. Utilizado para associar duas ou mais expressões, tornando-as obrigatórias no resultado da pesquisa.
or ou ||	Operador lógico OR. Utilizado para declarar duas ou mais expressões, fazendo com que, pelo menos uma, apareça no resultado da pesquisa.

O tcpdump utiliza outras expressões (# man tcpdump). Para agrupar operações lógicas, utilize parênteses protegidos com contra-barra. Exemplos:

Comando	Resultado
# tcpdump	Mostra todo o tráfego em modo promíscuous.
# tcpdump -i eth1 udp -X -s 1500	Mostra todo o tráfego UDP na eth1, em hexadecimal e ASCII. Captura até 1500 bytes por pacote. Resolve nomes (hosts e portas).
# tcpdump dst host 10.1.1.25 and udp -n	Mostra o cabeçalho de todo o tráfego destinado ao host 10.1.1.25 e que seja UDP. Não resolve nomes.
# tcpdump host 10.1.1.25 and udp and port 53	Mostra o cabeçalho de todo o tráfego oriundo ou destinado ao host 10.1.1.25, que seja UDP e que tenha como origem ou destino a porta 53. Resolve nomes.
# tcpdump host 10.1.1.25 and udp and port ! 53	Mostra o cabeçalho de todo o tráfego oriundo ou destinado ao host 10.1.1.25, que seja UDP e que tenha como origem ou destino qualquer porta, exceto a 53. Resolve nomes.
# tcpdump tcp and \(port 80 or port 110\)	Mostra o cabeçalho de todo o tráfego que seja TCP e que seja oriundo ou destinado às portas 80 ou 110. Resolve nomes.
# tcpdump icmp and host 10.1	Mostra os pacotes ICMP oriundos ou destinados a qualquer host que tenha o seu endereço IP iniciado com 10.1. Resolve nomes.
# tcpdump icmp and net 10.1.0.0/16	Mostra os pacotes ICMP oriundos ou destinados a qualquer host que pertança à rede 10.1.0.0 / 255.255.0.0. Resolve nomes.
# tcpdump ether host 00:c0:31:22:2d:11 -n	Mostra o cabeçalho de todo o tráfego destinado / oriundo do host com o endereço MAC especificado. Não resolve nomes.

3.6.5 tcpreplay

```
Instale com # apt-get install tcpreplay
```

O tcpreplay repete um tráfego salvo em um arquivo com formato tcpdump.

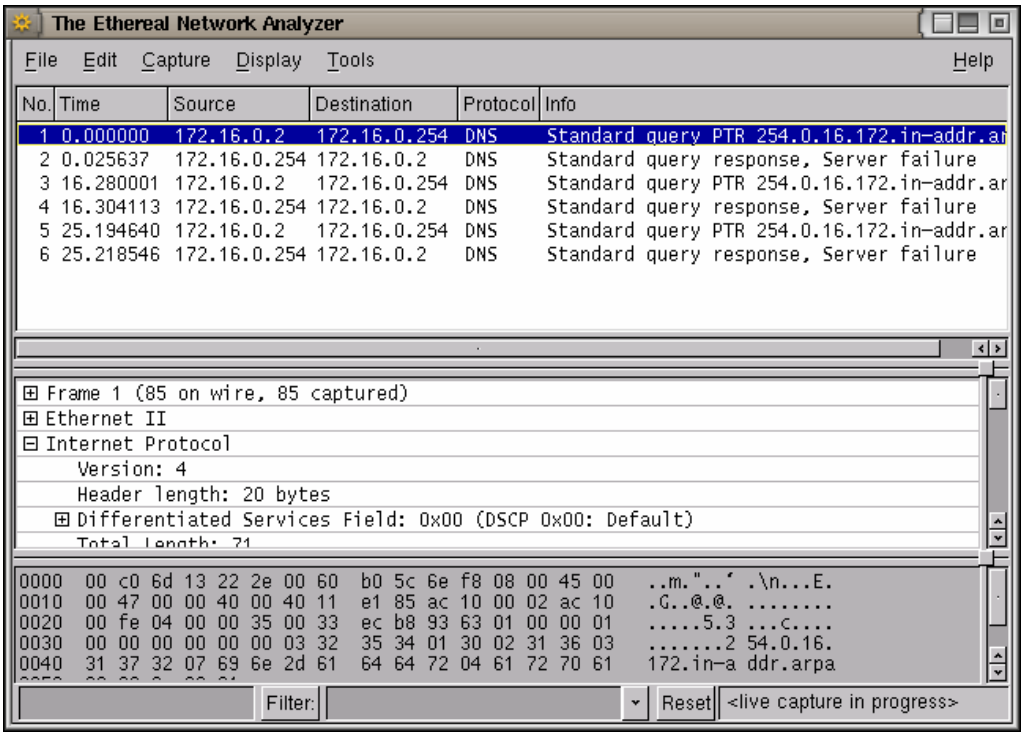
3.7 Analisadores avançados de tráfego

3.7.1 Ethereal (Wireshark)

```
Instale com # apt-get install wireshark
```

O Ethereal, recentemente rebatizado como Wireshark, é um programa para ambiente gráfico, compatível com o tcpdump, que fornece análises detalhadas do conteúdo dos pacotes. O

Ethereal lê e grava arquivos no formato tcpdump. A figura a seguir mostra um exemplo de análise de pacote:



3.7.2 tshark

```
Instale com # apt-get install tshark
```

O tshark é um programa para ambiente shell que faz uma análise de tráfego similar ao WireShark. A sintaxe utilizada é similar à do tcpdump. Para mais detalhes, utilize o comando # tshark -h.

3.8 Calculadoras IP

3.8.1 ipcalc

```
Instale com # apt-get install ipcalc.
```

Realiza o cálculo de redes, com máscaras inteiras ou quebradas. Exemplos:

```
# ipcalc 200.20.20.20/255.255.252.0
# ipcalc 200.20.20.20/17
```

3.8.2 sipcalc

```
Instale com # apt-get install sipcalc.
```

Similar ao ipcalc.