

Outros trabalhos em:
www.ProjetodeRedes.com.br

Introdução

Este trabalho tem como objetivo mostrar as funcionalidades do protocolo ICMP – (Internet Control Message Protocol), como um protocolo auxiliar ao protocolo IP enviando mensagens de erros para controle do IP e também como protocolo de gerenciamento do status dos ativos de rede como estações de trabalhos, switch's e roteadores através das suas duas principais aplicações, o Ping e o Traceroute ou Tracert (para windows).

O Protocolo ICMP

Existe um protocolo alternativo ao UDP para a transmissão de pequenas mensagens, chama-se ICMP (*Internet Control Message Protocol*) e é usado para a transmissão de mensagens de erro ou outras mensagens destinadas ao TCP/IP. Este protocolo não se destina a aplicações de utilizadores sendo usado somente para controlo de erro. Um exemplo deste protocolo surge quando num sistema Unix fazemos telnet à máquina A e recebemos a mensagem de erro - *host unreachable*, esta é uma mensagem ICMP a dizer que a máquina A não está disponível.

O ICMP é similar ao UDP pois utiliza mensagens que cabem num só datagrama, sendo no entanto ainda mais simples uma vez que não possui a indicação no seu cabeçalho dos portos de origem. As mensagens ICMP são interpretadas pelo software de rede pelo que não é necessário indicar os portos, o ICMP pode ainda ser usado para se obter informações acerca da rede. Para conhecer este protocolo com mais detalhe consultar o RFC 792.

Aplicações do ICMP

O ICMP possui duas aplicações muito populares:

1- Ping

Utilizado para verificar se um host está no ar. Envia datagramas IP com mensagens ICMP de Echo Reply, ou seja, requisitando uma resposta do host. Também mede o "round trip time", ou o tempo que o pacote leva para ir da máquina ao host e voltar. Na prática, supõe-se que, se o ping conseguiu resposta de um host, então outras aplicações como Telnet podem alcançar o host.

2- Traceroute

O Traceroute, que traduzido seria algo como "traçar a rota", é utilizado para descobrir a rota pela qual os datagramas IP passam, no caminho de um host a outro. Funciona de maneira interessante: o host que quer descobrir a rota envia um datagrama IP com o TTL (Time to Live) 1. Quando esse datagrama chega ao primeiro host da rota, este decremente o TTL, que passa a ser 0. Por isso, ele retorna uma mensagem ICMP de Time Exceeded para a origem do datagrama. Com isso, o host de origem já sabe qual é o primeiro host da rota. Esse processo pode ser facilmente repetido para TTLs maiores, como 2 para o segundo host, 3 para o terceiro, e assim por diante, até a chegada no host de destino.

Ferramentas ICMP

O protocolo *ICMP* - Internet Control Management Protocol - faz parte da pilha de protocolos *TCP/IP*, e está presente em todas as suas implementações. Ele consiste da troca de pacotes de controle com o objetivo de determinar acessibilidade, tempos de acesso (round-trip time) e rotas usadas para acesso entre máquinas.

Dois comandos bastante simples, que fazem uso extensivo de pacotes *ICMP*, são úteis em operações básicas de teste de acesso a hosts, e são muito usados por ferramentas de gerência: **ping** e **tracert**. Ver anexo 1 e 2 a sintaxe e opções dos comandos.

O comando ping

O comando **ping** permite verificar a acessibilidade de um host IP. Sua sintaxe básica é:
ping [options] host

O comando continuamente envia pacotes **ICMP** 'echo' (com normalmente 64 bytes) à máquina indicada, apresentando como saída o tempo necessário para receber a resposta do comando. Isso representa então o tempo de acesso "ida e volta" (round-trip) para acessar à máquina em questão. Um exemplo de saída:

```
sol:~> ping sunsite.unc.edu
PING sunsite.unc.edu (152.2.254.81) from 200.17.98.174 : 56 data bytes
64 bytes from 152.2.254.81: icmp_seq=0 ttl=242 time=424.2 ms
64 bytes from 152.2.254.81: icmp_seq=1 ttl=242 time=411.8 ms
64 bytes from 152.2.254.81: icmp_seq=2 ttl=242 time=531.0 ms
64 bytes from 152.2.254.81: icmp_seq=4 ttl=242 time=570.2 ms
64 bytes from 152.2.254.81: icmp_seq=5 ttl=242 time=547.2 ms
64 bytes from 152.2.254.81: icmp_seq=7 ttl=242 time=492.8 ms
64 bytes from 152.2.254.81: icmp_seq=8 ttl=242 time=404.4 ms
^C
--- sunsite.unc.edu ping statistics ---
23 packets transmitted, 16 packets received, 30% packet loss
round-trip min/avg/max = 404.4/485.3/570.2 ms
```

A listagem do comando **ping** é interrompida pelo ^C, e após a interrupção são apresentados alguns dados estatísticos relativos à conexão, como percentual de perda de pacotes e tempo médio de acesso.

O comando traceroute

O comando **traceroute** (**tracert** no Windows) permite determinar o caminho de acesso a uma máquina IP, a partir da máquina onde o comando está sendo executado. O caminho de acesso (rota) é uma seqüência de gateways (computadores e roteadores) pelos quais os pacotes atravessam para chegar ao destino. A sintaxe básica do comando é a seguinte:

```
traceroute [options] host
```

O comando **traceroute** determina a rota enviando pacotes UDP ao destino final, com valores de TTL (Time-To-Live) crescentes, iniciando em 1. O valor de TTL do pacote é decrementado a cada gateway, e quando chega em zero (0) ele é descartado e uma mensagem de erro *ICMP* 'time exceeded' é devolvida ao remetente. Assim, setando valores crescentes de TTL e interpretando as mensagens de erro *ICMP*, torna-se simples determinar a rota seguida pelos pacotes.

Uma saída típica do comando **traceroute** é a seguinte:

```

sol:~> /usr/sbin/traceroute www.unicamp.br
traceroute to obelix.unicamp.br (143.106.10.2), 30 hops max, 38 byte packets
 1 router (200.17.98.23) 1.041 ms 1.008 ms 1.266 ms
 2 10.19.74.29 (10.19.74.29) 7.640 ms * 3.209 ms
 3 bb2.pop-pr.rnp.br (200.19.74.20) 7.692 ms 5.404 ms 5.958 ms
 4 SP.serial-PR-SP.bb2.rnp.br (200.130.255.49) 13.872 ms 51.453 ms 44.270
ms
 5 ansp.ix.spo.ANSP.BR (200.136.34.1) 28.651 ms 43.421 ms 64.883 ms
 6 border2-e04-core.cas.ansp.br (143.106.99.9) 108.615 ms 75.864 ms
395.184 ms
 7 ansp-gw.unicamp.br (143.106.99.26) 130.609 ms 427.606 ms 85.641 ms
 8 * corp-gw.unicamp.br (143.106.2.52) 48.104 ms 71.590 ms
 9 obelix.unicamp.br (143.106.10.2) 53.521 ms * 112.220 ms

```

A primeira coluna indica o **valor de TTL** utilizado no pacote; em seguida é indicado o **nome do gateway** encontrado e seu número IP. Os valores indicados à direita correspondem aos **tempos de acesso** (round-trip time) para três testes consecutivos de acesso à máquina indicada na respectiva linha. Um asterisco (*) indica um time-out (não houve resposta no prazo default de 5 segundos do envio do pacote). Ver anexo 3 e 4.

Protocolo ICMP

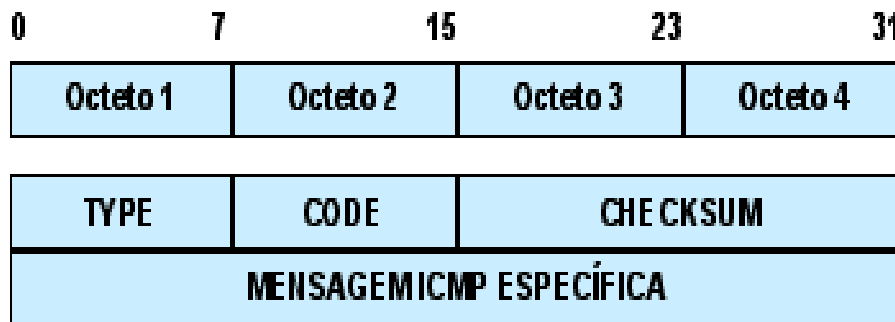
O protocolo ICMP é um protocolo auxiliar ao IP, que carrega informações de controle e diagnóstico, informando falhas como TTL do pacote IP expirou, erros de fragmentação, roteadores intermediários congestionados e outros.

Uma mensagem ICMP é encapsulada no protocolo IP, conforme ilustrado na figura abaixo. Apesar de encapsulado dentro do pacote IP, o protocolo ICMP não é considerado um protocolo de nível mais alto.



A mensagem ICMP é sempre destinada ao host origem da mensagem, não existindo nenhum mecanismo para informar erros aos roteadores no caminho ou ao host destino.

As mensagens ICMP possuem um identificador principal de tipo (TYPE) e um identificador de sub-tipo (CODE), conforme pode ser visto no formato de mensagem ilustrado abaixo.



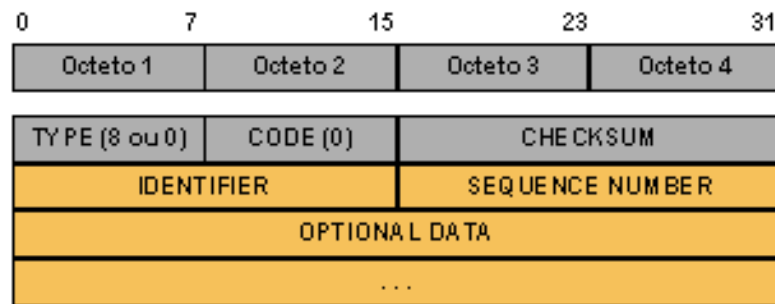
Os tipos de mensagem ICMP são listados na tabela abaixo:

Tipo	Mensagem ICMP	Categoria
0	Echo Reply	Controle
3	Destination Unreachable	Erro
4	Source Quench	Controle
5	Redirect	Controle
8	Echo Request	Controle
9	Router Advertisement (RFC 1256)	Controle
10	Router Solicitation (RFC 1256)	Controle
11	Time Exceeded for a Datagram	Erro
12	Parameter Problem on a Datagram	Erro
13	Timestamp Request	Controle
14	Timestamp Reply	Controle
15	Information Request (obsoleto)	Controle
16	Information Reply (obsoleto)	Controle
17	Address Mark Request	Controle
18	Address Mark Reply	Controle

As mensagens ICMP são listadas abaixo:

Echo Request e Echo Reply

Utilizada pelo comando ping, a mensagem Echo Request enviada para um host causa o retorno de uma mensagem Echo Reply. É utilizada principalmente para fins de testes de conectividade entre as duas máquinas.



Destination Unreachable

Esta mensagem possui diversos sub-tipos para identificar o motivo da não alcançabilidade: os sub-tipos utilizados atualmente são:

0 : Network Unreachable - Rede destino inalcançável

1 : Host Unreachable (ou falha no roteamento para subnet) - Máquina destino inalcançável

2 : Protocol Unreachable - Protocolo destino desativado ou aplicação inexistente

3 : Port Unreachable - Porta destino sem aplicação associada

4 : Fragmentation Needed and DNF set - Fragmentação necessária mas bit DNF setado. Alterado também pela RFC 1191 para suporta o protocolo Path MTU Discovery

5 : Source Route Failed - Roteamento por rota especificada em opção IP falhou

6 : Destination Network Unknown

7 : Destination Host Unknown

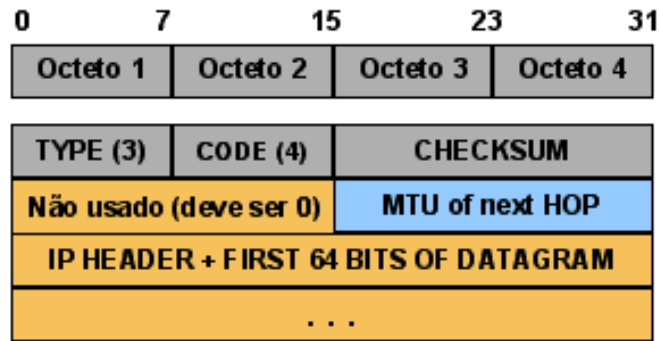
8 : Source Host Isolated

9 : Communication with destination network administratively prohibited

10 : Communication with destination host administratively prohibited

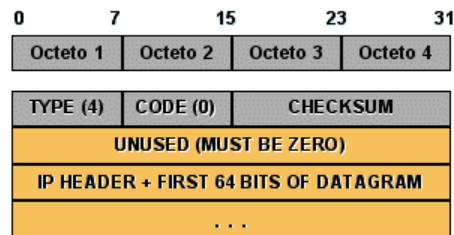
O sub-tipo Fragmentation Needed and DNF set é utilizado como forma de um host descobrir o menor MTU nas redes que serão percorridas entre a origem e o destino. Por meio desta mensagem, é possível enviar pacotes que não precisarão ser fragmentados, aumentando a eficiência da rede. Esta técnica, que forma um protocolo é denominado de ICMP MTU Discovery Protocol, definido na RFC 1191.

A operação é simples. Todo pacote IP enviado é marcado com o bit DNF (Do Not Fragment), que impede sua fragmentação nos roteadores. Desta forma, se uma pacote IP, ao passar por um roteador para chegar a outra rede com MTU menor, deva ser fragmentado, o protocolo IP não irá permitir e enviará uma mensagem ICMP Destination Unreachable para o destino. Para suportar esta técnica, a mensagem ICMP foi alterada para informar o MTU da rede que causou o ICMP. Desta forma, a máquina origem saberá qual o valor de MTU que causou a necessidade de fragmentação, podendo reduzir o MTU de acordo, nos próximos pacotes. Esta mensagem está ilustrada na figura abaixo.



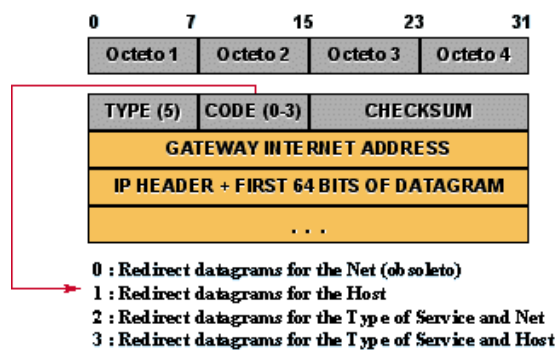
Source Quench

Esta mensagem é utilizada por um roteador para informar à origem, que foi obrigado a descartar o pacote devido a incapacidade de roteá-lo devido ao tráfego.

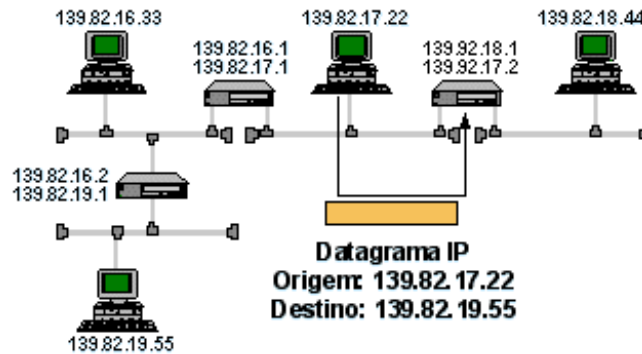


Redirect

Esta mensagem, uma das mais importantes do protocolo IP, é utilizada por um roteador para informar ao host origem de uma mensagem que existe uma rota direta mais adequada através de outro roteador. O host, após receber a mensagem ICMP, instalará uma rota específica para aquele host destino:



A operação do ICMP Redirect ocorre conforme os diagramas abaixo. Note que a rota instalada é uma rota específica para host, com máscara 255.255.255.255, não servindo para outras máquinas na mesma rede. Se uma máquina se comunica com 10 máquinas em outra rede e se basear em ICMP Redirect para aprender as rotas, ele instalará pelo menos 10 entradas na tabela de rede, uma para cada máquina

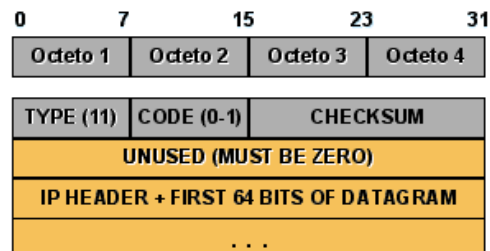


Na figura acima, a estação 139.82.17.22 instalou, após a mensagem ICMP, a seguinte rota na tabela de rotas:

Rede Destino	Máscara	Roteador (Gateway)	Hops
139.82.19.55	255.255.255.255	139.82.17.1	0

TTL Expired

Esta mensagem ICMP originada em um roteador informa ao host de origem que foi obrigado a descartar o pacote, uma vez que o TTL chegou a zero.



Esta mensagem é utilizada pelo programa traceroute (ou tracert no Windows) para testar o caminho percorrido por um pacote. O programa funciona da seguinte forma:

1. É enviada uma mensagem ICMP Echo Request para um endereço IP destino. Esta mensagem é enviada com TTL = 1.
2. Quando chega ao primeiro roteador, este decrementa o valor de TTL da mensagem IP e retorna uma mensagem ICMP TTL Expired. O programa armazena o endereço IP do roteador que enviou a mensagem TTL Expired.
3. O programa envia outra mensagem ICMP Echo Request para o endereço IP destino. Esta mensagem é enviada desta vez com TTL=2.
4. A mensagem atravessa o primeiro roteador e tem o TTL decrementado para 1. Quando chega ao segundo roteador, o TTL torna-se 0 e este roteador envia uma mensagem ICMP TTL Expired para a máquina origem. Esta armazena o endereço do segundo roteador.
5. Esta operação prossegue até que a máquina destino responda. Todos os roteadores no caminho são registrados.

Note, entretanto, que devido à diferenças de rotas seguidas pelos diversos pacotes, o caminho obtido não necessariamente é único. A execução do programa traceroute mais de uma vez pode revelar rotas diferentes seguidas pelos pacotes.

ICMP Router Solicitation/Advertisement

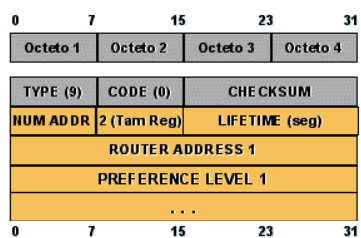
Esta variação de ICMP, definido na RFC 1256 foi projetada para permitir que um roteador possa divulgar sua existência para as máquinas existentes na rede. O objetivo desta função é evitar a necessidade de se configurar manualmente todas as estações da rede com a rota default e permitir que uma estação conheça outros roteadores além do default que possam rotear no caso de falha do principal.

A mensagem é composta de duas formas: a solicitação de divulgação de uma roteador e o anúncio de um roteador. O roteador pode ser configurado para enviar automaticamente as mensagens de anúncio ou fazê-lo apenas comandado por uma mensagem de solicitação.

A mensagem ICMP Router Solicitation é mostrada abaixo.



A mensagem ICMP Router Advertisement é mostrada abaixo.



Esta mensagem pode conter a divulgação de diversos roteadores iniciada a partir de um que seja configurado para divulgá-los. O número de preferência é a ordem de preferência que estes roteadores podem ser utilizados pelas estações.

Conclusão

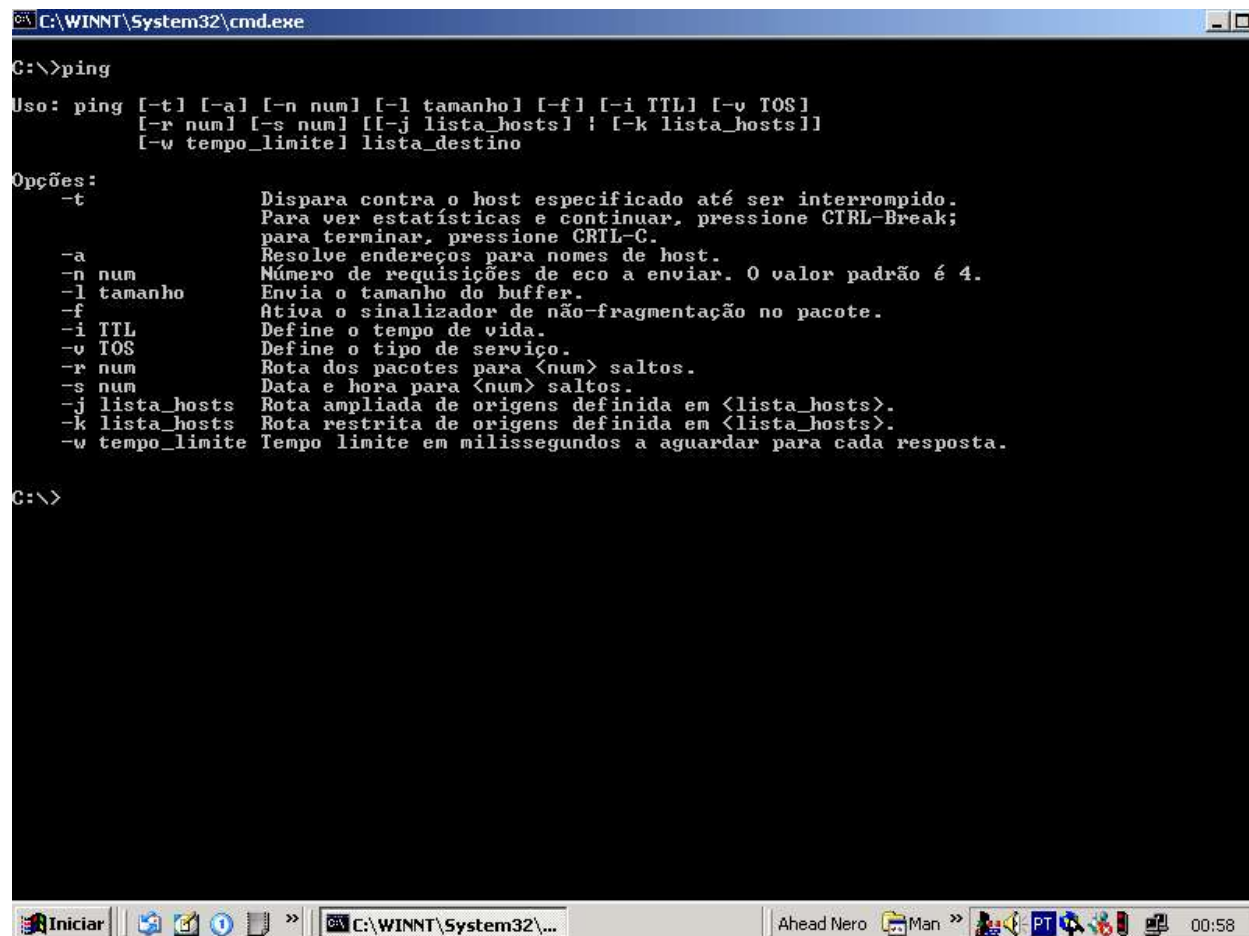
O trabalho sobre a pesquisa do protocolo ICMP demonstrou os conhecimentos sobre como os pacotes icmp são úteis para o protocolo Ip auxiliando com suas ferramentas ping e traceroute ou tracert, sendo indispensável na maioria das ferramentas de monitoração de redes locais e utilizados por diversos analisadores de redes e gerenciamentos de elementos de redes como roteadores com suas funções de verificações de status de atividade e traçando rotas.

Bibliografia

RFC 792. Internet Control Message Protocol. URL: <http://www.ietf.org>.

Variados site da internet encontrados através: <http://www.google.com>

Anexo 1 opções do comando ping.



```
C:\WINNT\System32\cmd.exe

C:\>ping

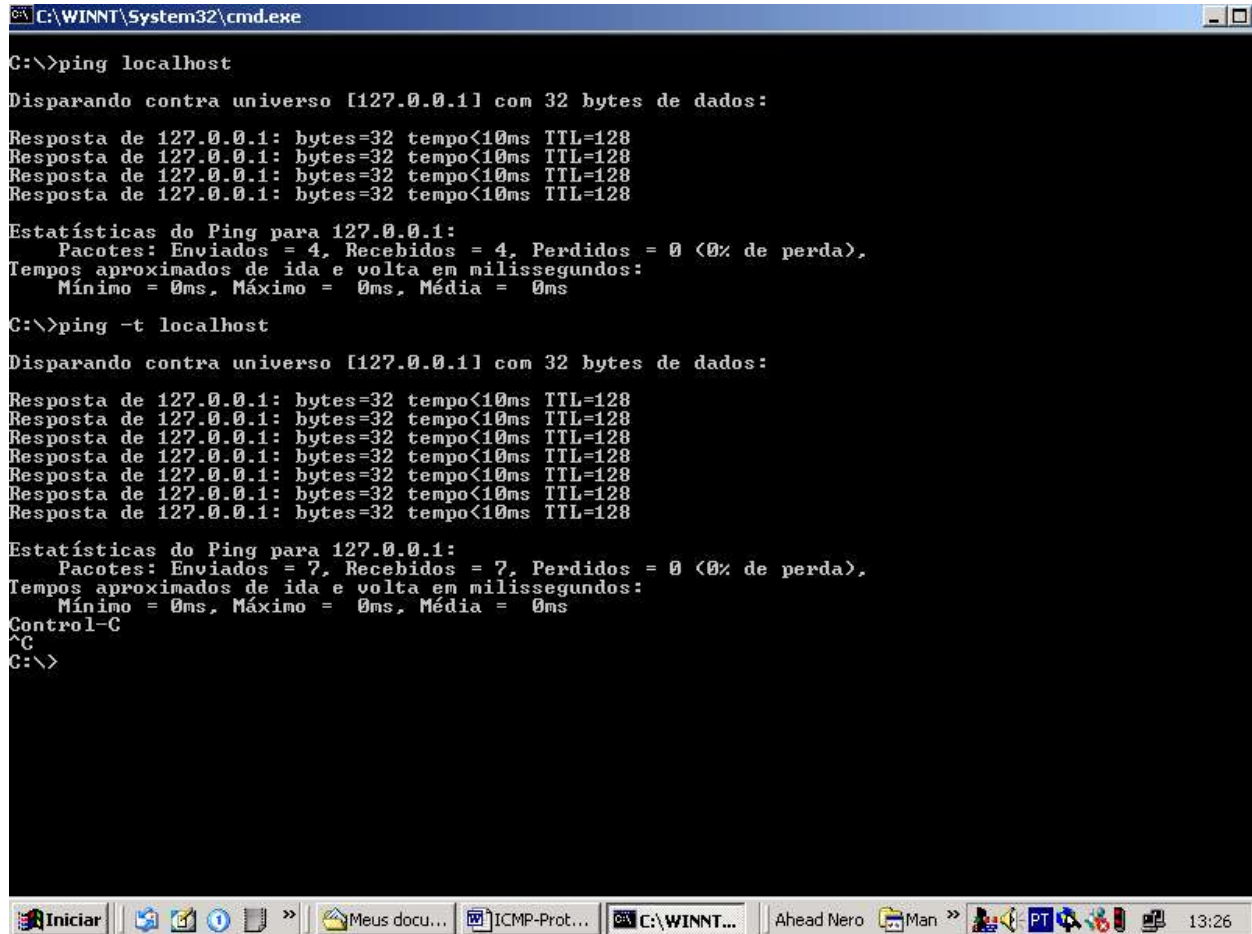
Uso: ping [-t] [-a] [-n num] [-l tamanho] [-f] [-i TTL] [-v TOS]
        [-r num] [-s num] [[-j lista_hosts] | [-k lista_hosts]]
        [-w tempo_limite] lista_destino

Opções:
-t          Dispara contra o host especificado até ser interrompido.
            Para ver estatísticas e continuar, pressione CTRL-Break;
            para terminar, pressione CTRL-C.
-a          Resolve endereços para nomes de host.
-n num     Número de requisições de eco a enviar. O valor padrão é 4.
-l tamanho Envia o tamanho do buffer.
-f          Ativa o sinalizador de não-fragmentação no pacote.
-i TTL     Define o tempo de vida.
-v TOS     Define o tipo de serviço.
-r num     Rota dos pacotes para <num> saltos.
-s num     Data e hora para <num> saltos.
-j lista_hosts Rota ampliada de origens definida em <lista_hosts>.
-k lista_hosts Rota restrita de origens definida em <lista_hosts>.
-w tempo_limite Tempo limite em milissegundos a aguardar para cada resposta.

C:\>
```

The screenshot shows a Windows command prompt window with the title bar "C:\WINNT\System32\cmd.exe". The user has entered the command "ping". The command prompt displays the usage and options for the ping command. The options listed are: -t (continuous ping), -a (resolve addresses), -n num (number of requests), -l tamanho (buffer size), -f (no fragmentation), -i TTL (time to live), -v TOS (type of service), -r num (route hops), -s num (timestamp hops), -j lista_hosts (loose source route), -k lista_hosts (strict source route), and -w tempo_limite (wait time). The window's taskbar at the bottom shows the "Iniciar" button, several icons, and the system clock displaying "00:58".

Anexo 2 sintaxe do comando ping.



```
C:\WINNT\System32\cmd.exe

C:\>ping localhost

Disparando contra universo [127.0.0.1] com 32 bytes de dados:

Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128

Estatísticas do Ping para 127.0.0.1:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
    Tempos aproximados de ida e volta em milissegundos:
        Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\>ping -t localhost

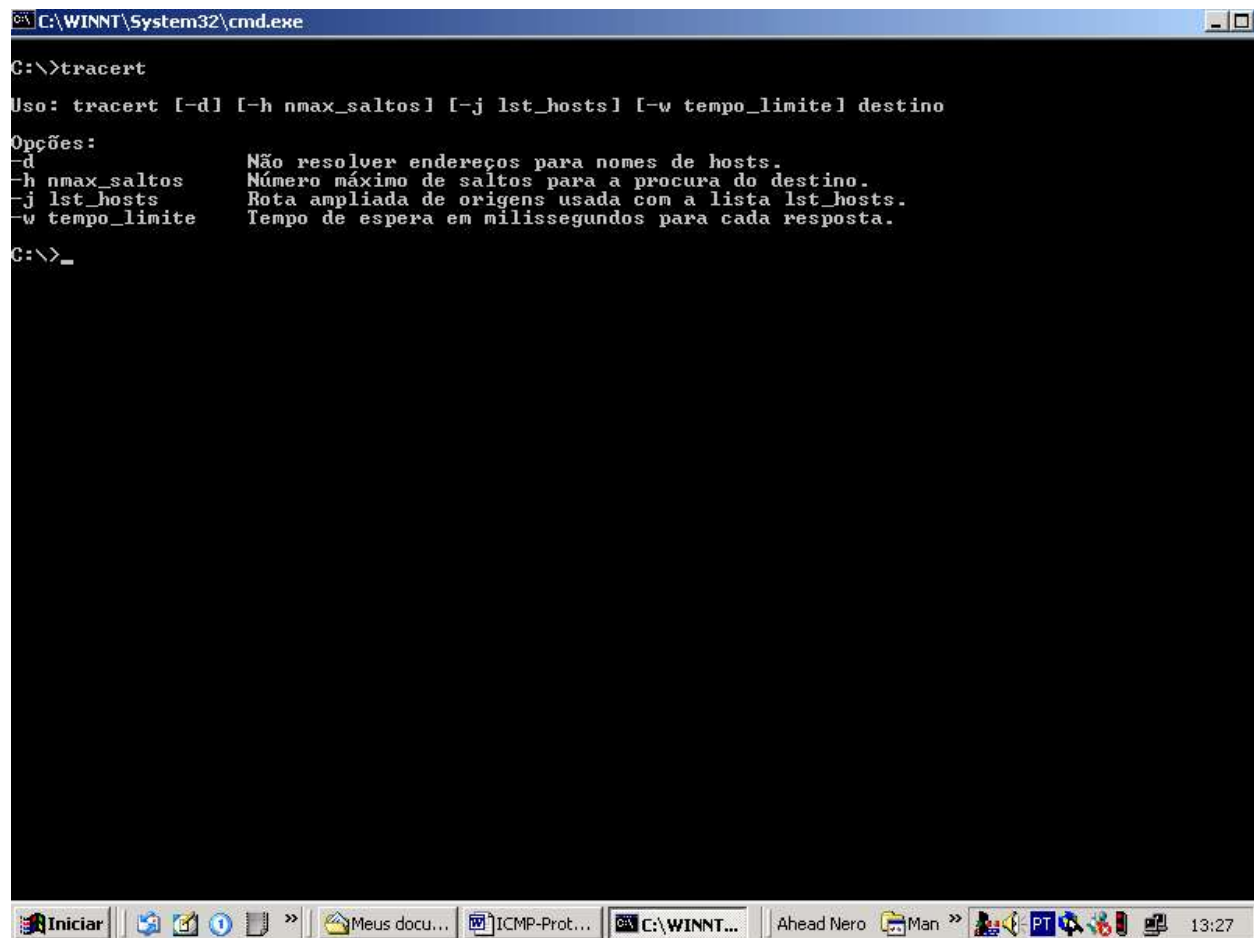
Disparando contra universo [127.0.0.1] com 32 bytes de dados:

Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128
Resposta de 127.0.0.1: bytes=32 tempo<10ms TTL=128

Estatísticas do Ping para 127.0.0.1:
    Pacotes: Enviados = 7, Recebidos = 7, Perdidos = 0 (0% de perda),
    Tempos aproximados de ida e volta em milissegundos:
        Mínimo = 0ms, Máximo = 0ms, Média = 0ms
Control-C
^C
C:\>
```

The screenshot shows a Windows command prompt window titled "C:\WINNT\System32\cmd.exe". The user has entered the command "ping localhost", which returns four successful responses from 127.0.0.1 with 0ms round-trip times. Then, the user enters "ping -t localhost", which starts a continuous ping loop. The first seven responses are shown, all successful with 0ms round-trip times. The user then presses "Control-C" (indicated by "^C"), which stops the continuous ping. The prompt returns to "C:\>". The taskbar at the bottom shows the "Iniciar" button and several open applications, including "Meus docu...", "ICMP-Prot...", "C:\WINNT...", "Ahead Nero", and "Man". The system clock shows 13:26.

Anexo 3 opções do comando tracert.



```
C:\WINNT\System32\cmd.exe

C:\>tracert

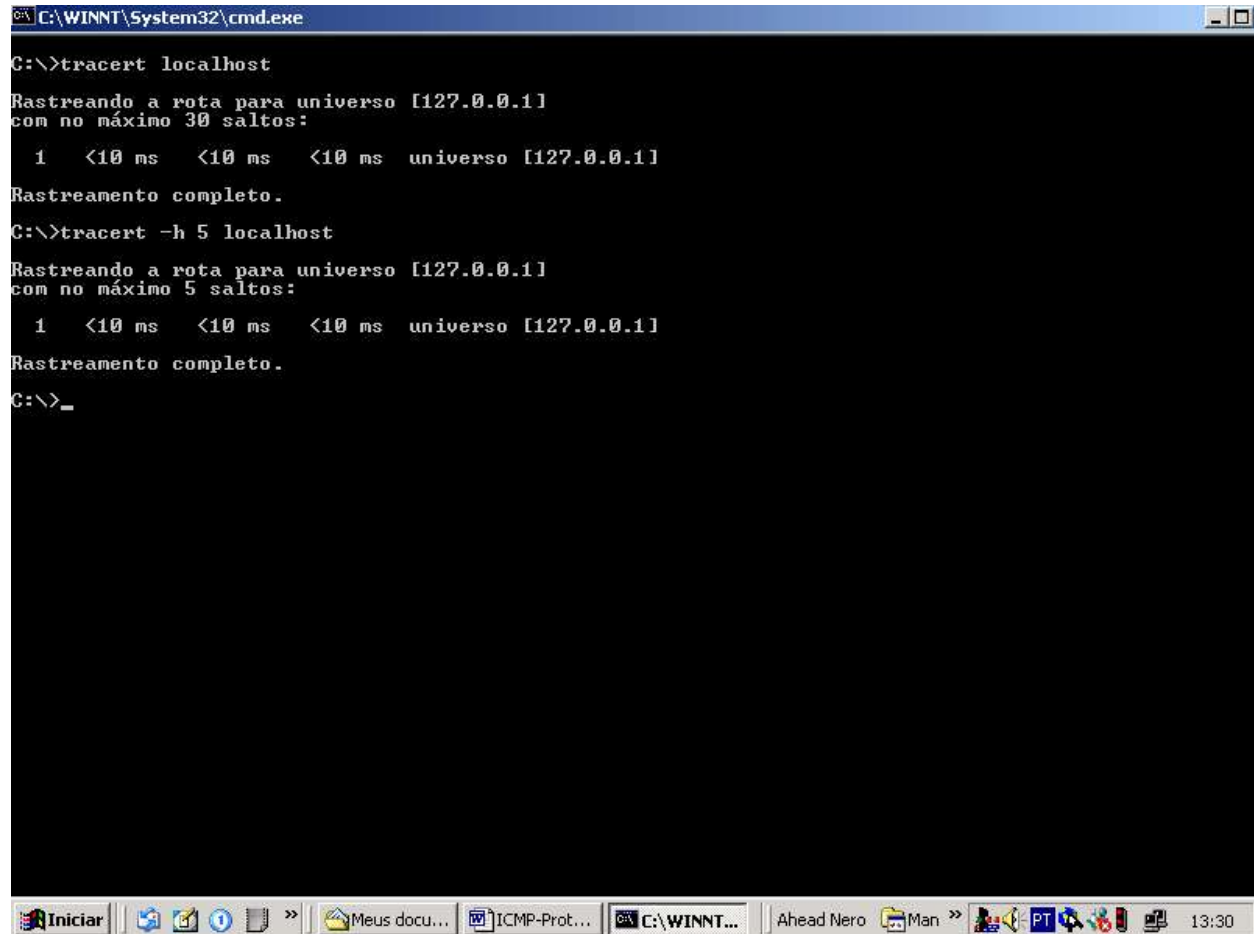
Uso: tracert [-d] [-h nmax_saltos] [-j lst_hosts] [-w tempo_limite] destino

Opções:
-d          Não resolver endereços para nomes de hosts.
-h nmax_saltos  Número máximo de saltos para a procura do destino.
-j lst_hosts    Rota ampliada de origens usada com a lista lst_hosts.
-w tempo_limite  Tempo de espera em milissegundos para cada resposta.

C:\>_
```

The screenshot shows a Windows command prompt window with the title bar 'C:\WINNT\System32\cmd.exe'. The command 'tracert' has been entered, and the help text is displayed. The help text includes the usage 'Uso: tracert [-d] [-h nmax_saltos] [-j lst_hosts] [-w tempo_limite] destino' and a list of options: '-d' for not resolving host addresses, '-h nmax_saltos' for the maximum number of hops, '-j lst_hosts' for the list of source addresses, and '-w tempo_limite' for the timeout in milliseconds. The prompt 'C:\>_' is shown at the bottom of the command window. The taskbar at the bottom of the screen shows several open applications: 'Iniciar', 'Meus docu...', 'ICMP-Prot...', 'C:\WINNT...', 'Ahead Nero', and 'Man', along with system icons and the time '13:27'.

Anexo 4 sintaxe do comando tracert



```
C:\WINNT\System32\cmd.exe

C:\>tracert localhost

Rastreando a rota para universo [127.0.0.1]
com no máximo 30 saltos:

  1  <10 ms  <10 ms  <10 ms  universo [127.0.0.1]

Rastreamento completo.

C:\>tracert -h 5 localhost

Rastreando a rota para universo [127.0.0.1]
com no máximo 5 saltos:

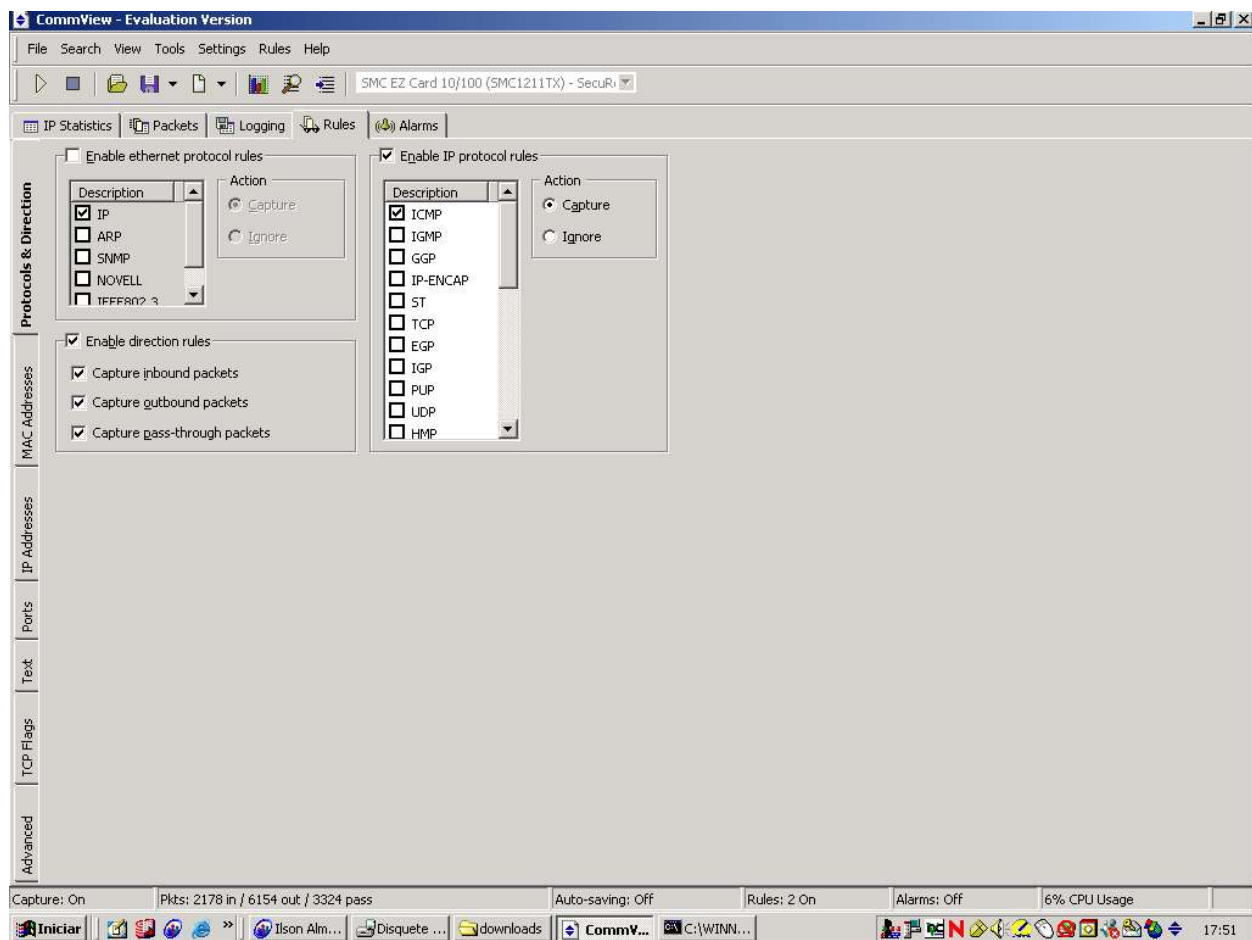
  1  <10 ms  <10 ms  <10 ms  universo [127.0.0.1]

Rastreamento completo.

C:\>_
```

The screenshot shows a Windows XP desktop with a taskbar at the bottom. The taskbar includes the 'Iniciar' button, several icons, and open application windows: 'Meus docu...', 'ICMP-Prot...', 'C:\WINNT...', 'Ahead Nero', and 'Man'. The system clock shows 13:30. The command prompt window is titled 'C:\WINNT\System32\cmd.exe' and displays the output of the 'tracert' command for 'localhost' and 'localhost -h 5'. Both commands show a single hop to the 'universo [127.0.0.1]' with a response time of less than 10 ms. The window title bar has standard minimize, maximize, and close buttons.

Anexo 5 Configuração do connview.



Anexo 5 connview ping.

CommView - Evaluation Version

File Search View Tools Settings Rules Help

SMC EZ Card 10/100 (SMC1211TX) - SecuR...

IP Statistics Packets Logging Rules Alarms

No	Protocol	MAC Addresses	IP Addresses	Ports	Delta
3	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	24,297
4	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,015
5	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.16.100		N/A	0,000
6	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,985
7	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,015
8	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.16.100		N/A	0,000
12	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,985
13	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,015
14	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.16.100		N/A	0,000
15	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,985
16	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.16.100		N/A	0,015
17	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.16.100		N/A	0,000

0x0000 00 10 B5 F4 94 44 00 01-30 2C FE 00 08 00 45 00 ..µ6"D...0,p...E.
0x0010 00 3C 5F 0C 00 00 1C 01-41 C8 0A 3D 10 64 0A 3D .<_.....AB.=.d.=
0x0020 D9 0F 00 00 EB 58 02 00-68 03 61 62 63 64 65 66 U...eX...h.abcdef
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76 ghijklmnopqrstuv
0x0040 77 61 62 63 64 65 66 67-68 69 wabcde fghi

Protocol: 0x01 (1) - ICMP
Checksum: 0x41C8 (16840) - correct
Source IP: 10.61.16.100
Destination IP: 10.61.217.15
IP Options: None
ICMP
Type: 0x00 (0) - Echo reply
Code: 0x00 (0)
Checksum: 0xEB58 (60248) - correct
Identifier: 0x0200 (512)
Sequence Number: 0x6803 (26627)

Capture: On Pkts: 2046 in / 5800 out / 3245 pass Auto-saving: Off Rules: 2 On Alarms: Off 3% CPU Usage

Iniciar Ilson Almeid... Disquete de ... downloads CommView... C:\WINNT\s... 17:47

Anexo 6 connview tracert

The screenshot displays the CommView - Evaluation Version interface. The top menu bar includes File, Search, View, Tools, Settings, Rules, and Help. Below the menu is a toolbar with various icons. The main window is divided into several sections:

- IP Statistics:** A table showing packet capture details.
- Packets:** A detailed view of the selected packet (No. 286).
- Logging:** A section for logging configuration.
- Rules:** A section for rule configuration.
- Alarms:** A section for alarm configuration.

The **IP Statistics** table contains the following data:

No	Protocol	MAC Addresses	IP Addresses	Ports	Delta
246	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,140	
247	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,000	
248	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	
249	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	
250	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,000	
251	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	
252	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	
253	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,000	
286	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,125	
299	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,969	
302	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,734	
305	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,766	
308	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,531	
311	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.217.1	N/A	0,969	
312	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	1,516	
313	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,015	
314	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.250.97	N/A	0,000	
315	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	
316	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,063	
317	IP/ICMP	00:10:B5:F4:94:44 <= 00:01:30:2...10.61.217.15 <= 10.61.250.97	N/A	0,000	
318	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	
319	IP/ICMP	00:10:B5:F4:94:44 => 00:01:30:2...10.61.217.15 => 10.61.32.211	N/A	0,000	

Below the table, a message states: "THIS EVALUATION VERSION DISPLAYS ONLY HALF OF THE PACKETS".

The **Packets** section shows a detailed view of the selected packet (No. 286):

- IP Options:** None
- ICMP:**
 - Type: 0x03 (3) - Destination unreachable
 - Code: 0x03 (3) - Port unreachable
 - Checksum: 0xFBC4 (64452) - correct
- Original packet:**
 - IP:**
 - UDP:**
 - Source port: 137
 - Destination port: 137
 - Length: 0x003A (58)
 - Checksum: 0x0000 (0) - not computed

The bottom status bar shows: Capture: On, Pkts: 2269 in / 6368 out / 3394 pass, Auto-saving: Off, Rules: 2 On, Alarms: Off, 3% CPU Usage. The taskbar at the bottom includes icons for various applications and the system clock showing 17:54.

Outros trabalhos em:
www.ProjetodeRedes.com.br