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 gerênciamento do status dos ativos de rede como estações de trabalhos, switch´s e roteadores através das suas duas principais aplicações, o Ping e o Tracerroute 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 que a máquina A não está disponivel.
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 "roud 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 traduzio 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 decrementa 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* ***traceroute****. 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
```

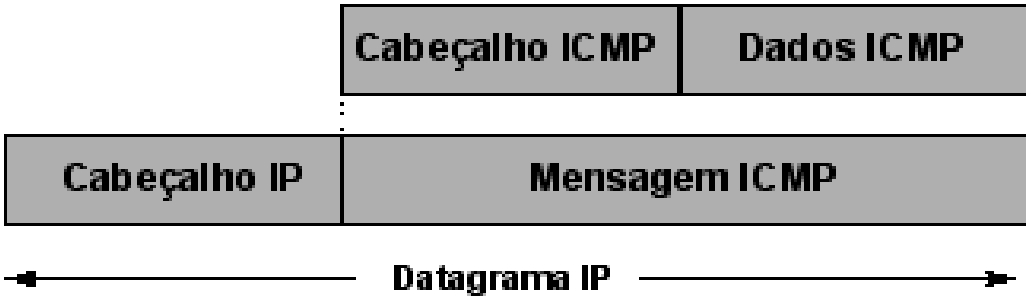
O comando ***traceroute*** *determina a rota enviando pacotes UDP ao destino final, com valores de TTL (*Time-To-Live*) crescentes, iniciando em 1. O valor de TTL do pacote é decrementado a cada gateway, e quando chega em zero (0) ele é descartado e uma mensagem de erro ICMP 'time exceeded' é devolvida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

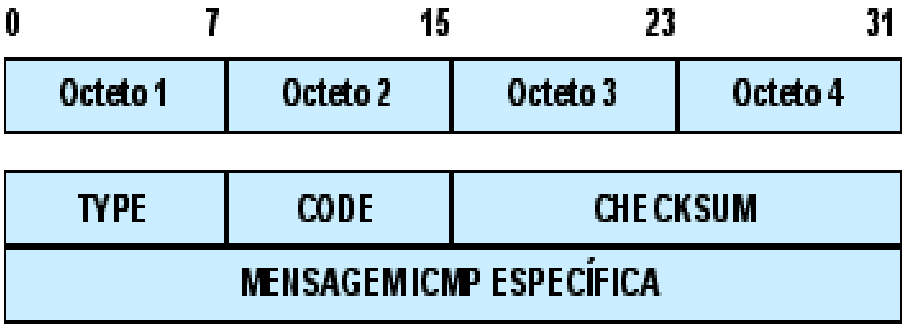
Protocolo ICMP

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



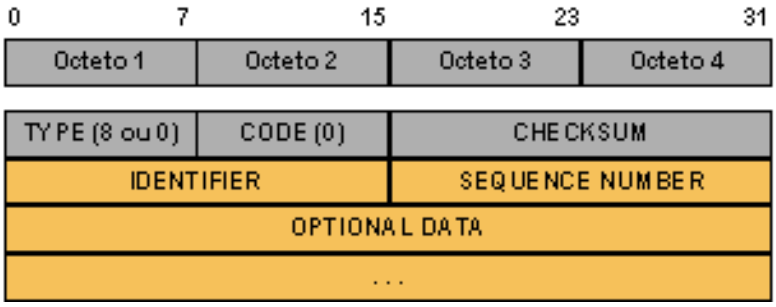
Os tipos de mensagem ICMP são listados na tabela abaixo:

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 (osboleto)*	*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

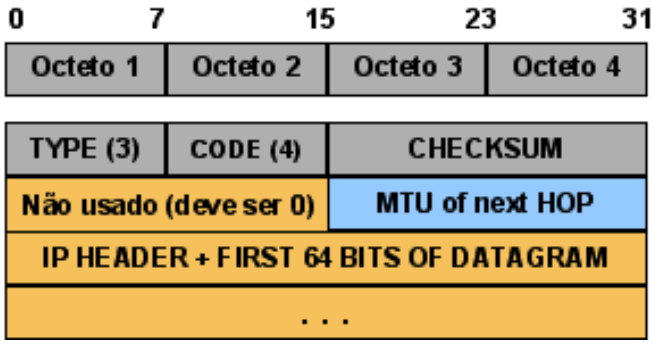
Utilizada pelo comando ping, a mensagem Echo Request enviada para um host causa o retorno de uma mensagem Echo Reply. É utilizada principalmente para fins de testes de conectividade entre as duas máquinas.



Destination Unreacheable
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*

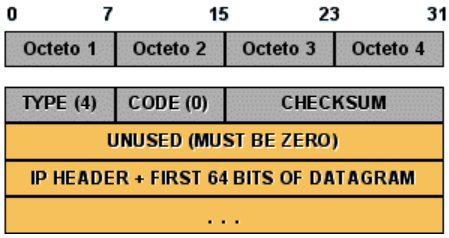
***5 : Source Route Failed** - Roteamento por rota especificada em opção IP falhou*
6 : Destination Network Unknown
7 : Destination Host Unknown
8 : Source Host Isolated
9 : Communication with destination network administratively prohibited
10 : Communication with destination host administratively prohibited

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 Unreacheable 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.



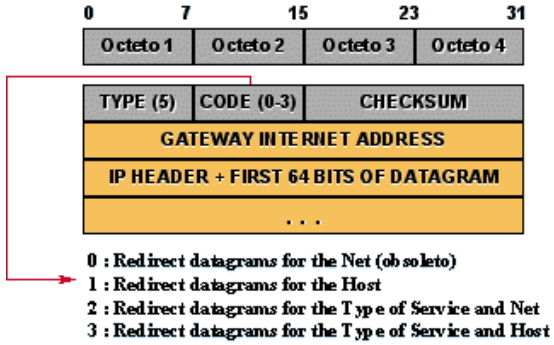
Source Quench

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.

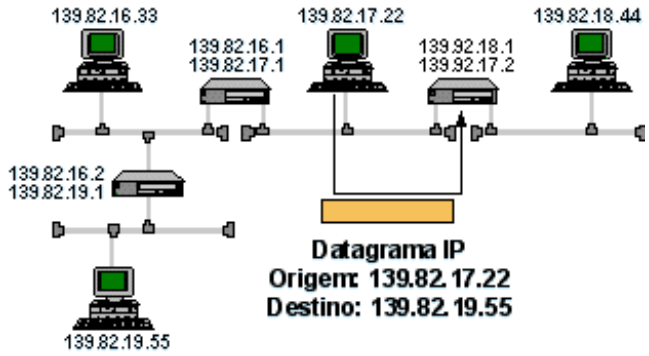


Redirect

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

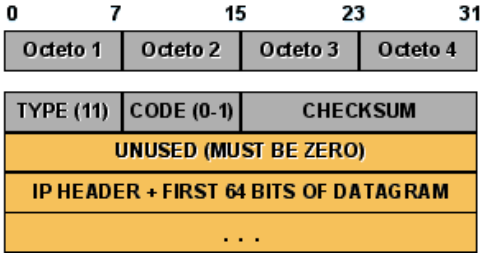


Na figura acima, a estação 139.82.17.22 instalou, após a mensagem ICMP, a seguinte rota na tabela de rotas:

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.

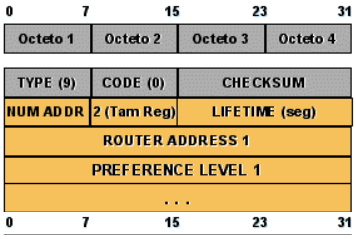
ICMP Router Solicitation/Advertisement

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

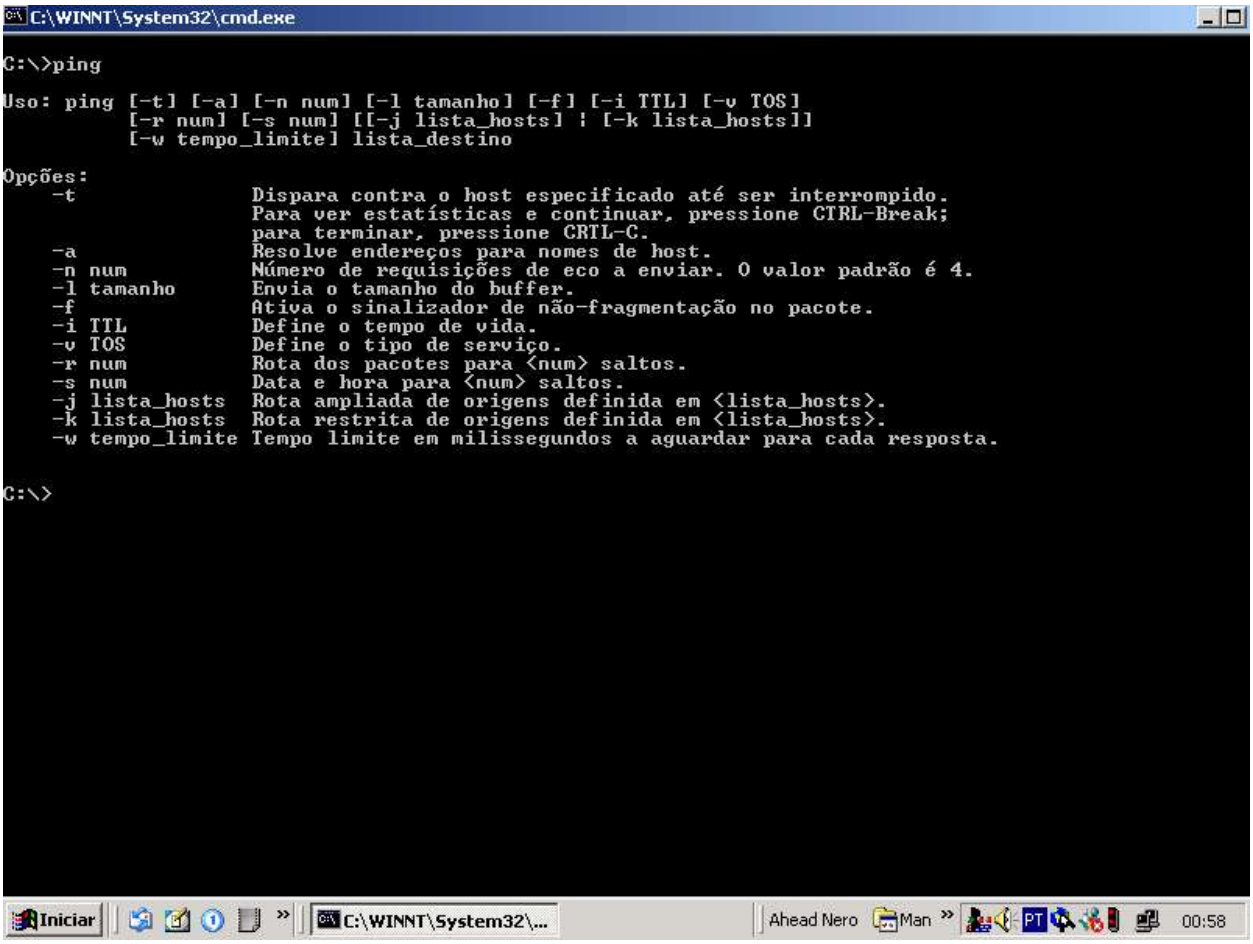
O trabalho sobre a pesquisa do protocolo ICMP demostrou os conhecimentos sobre como os pacotes icmp são úteis para o protocolo Ip auxiliando com suas ferramentas ping e tracerroute ou tracert, sendo indispensável na maioria das ferramentas de monitoração de redes locais e utilizados por diversos analisadores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

Bibliografia

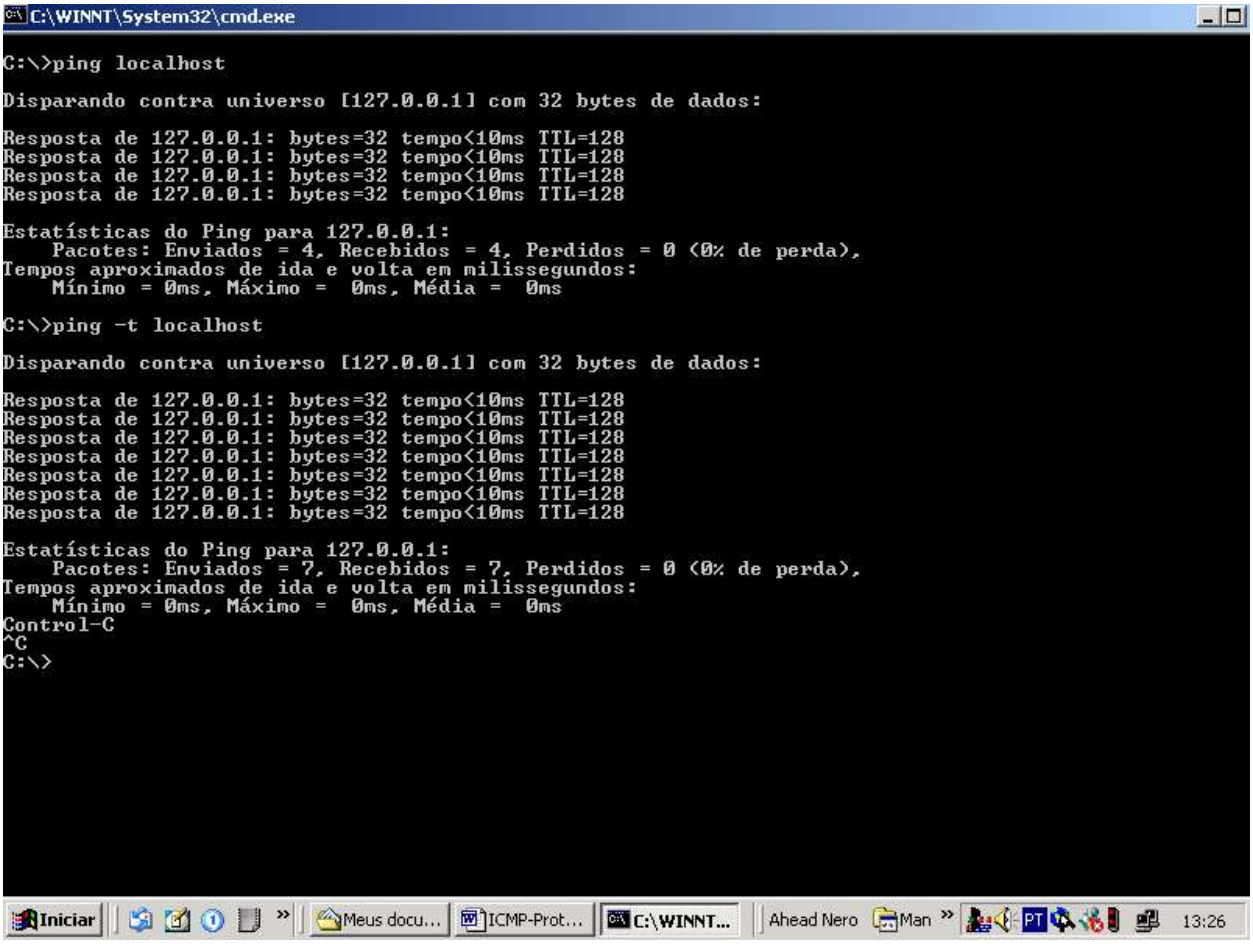
RFC 792. Internet Control Messagem Protocol. URL: http://www.ietf.org.

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

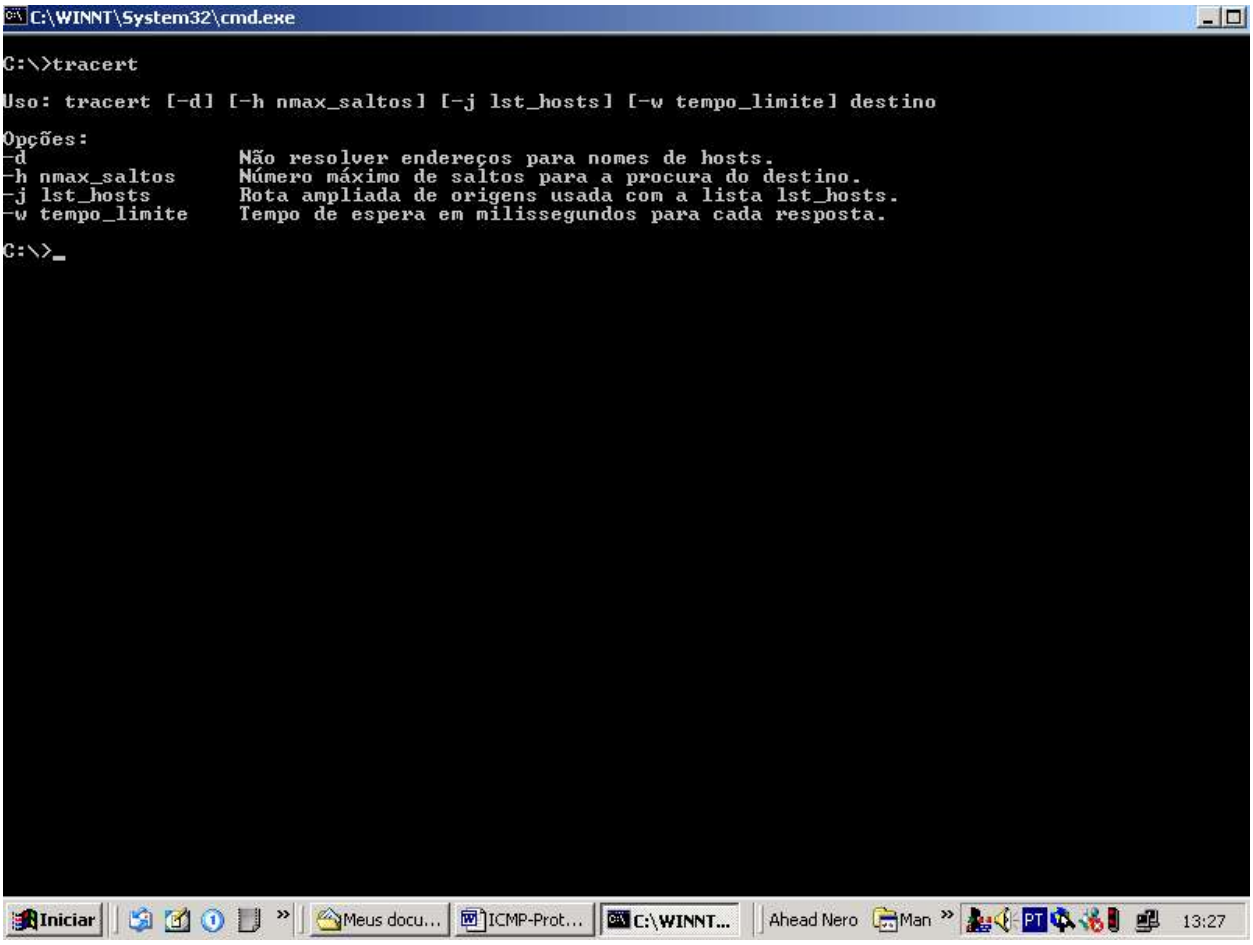
Anexo 1 opções do comando ping.



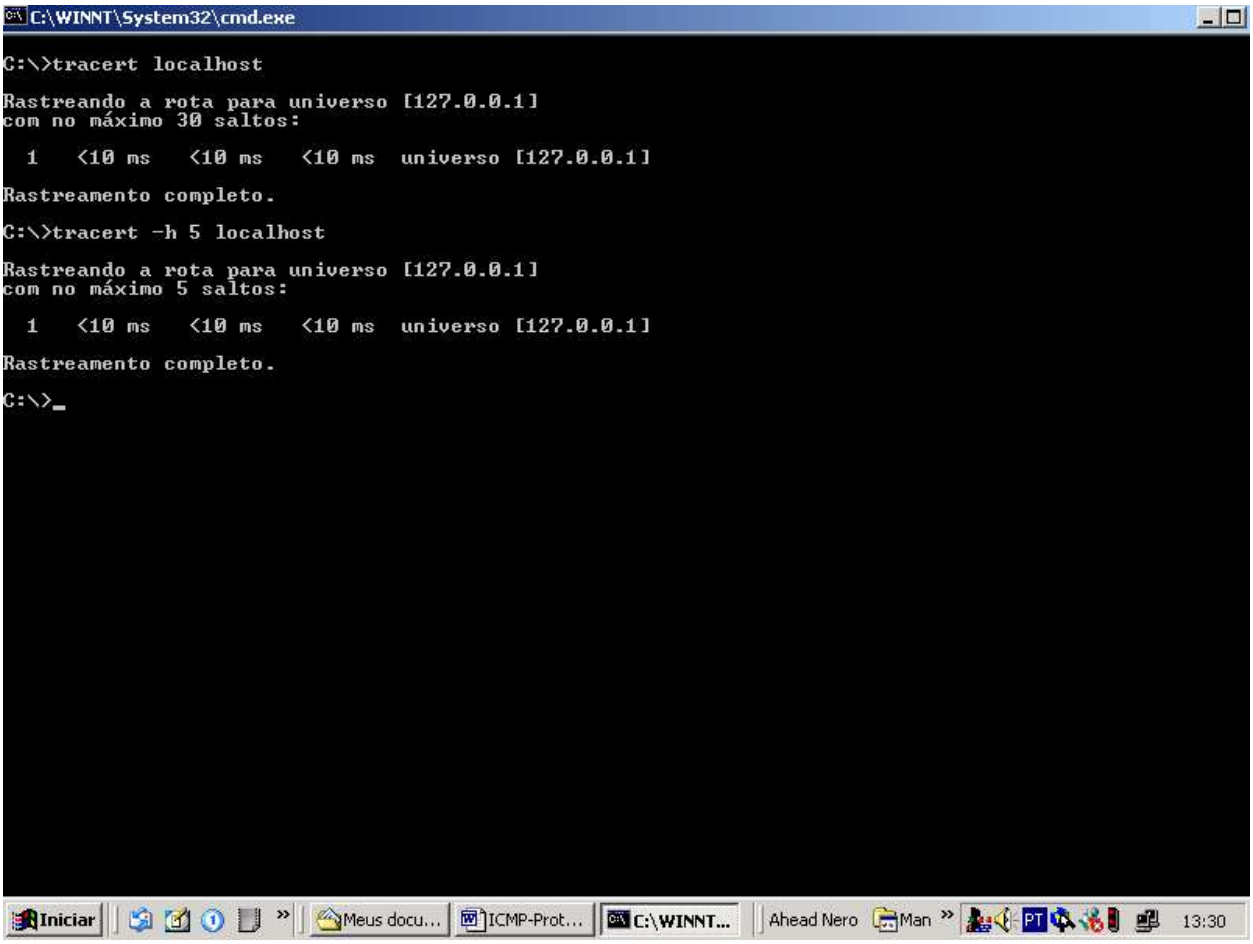
Anexo 2 sintaxe do comando ping.



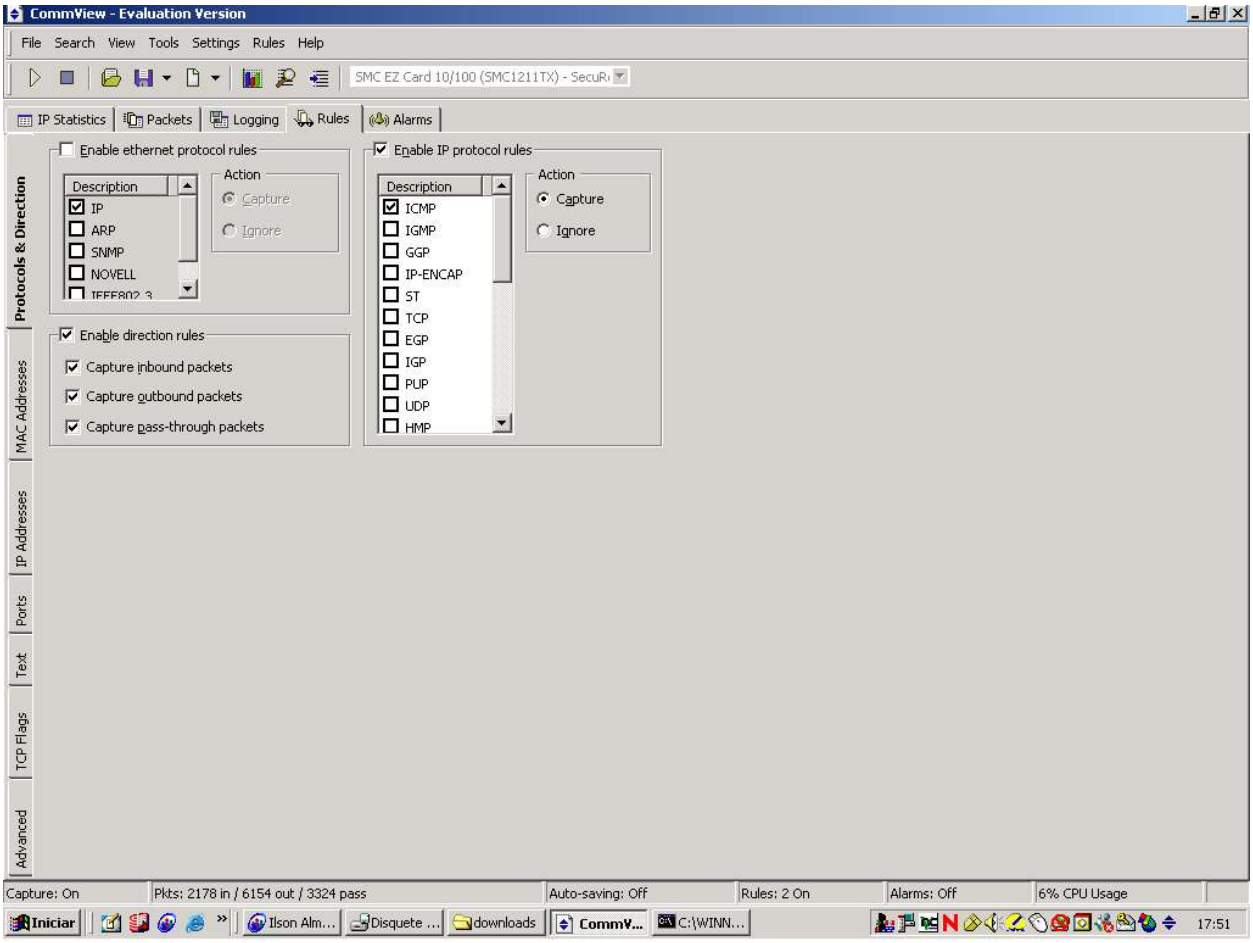
Anexo 3 opções do comando tracert.



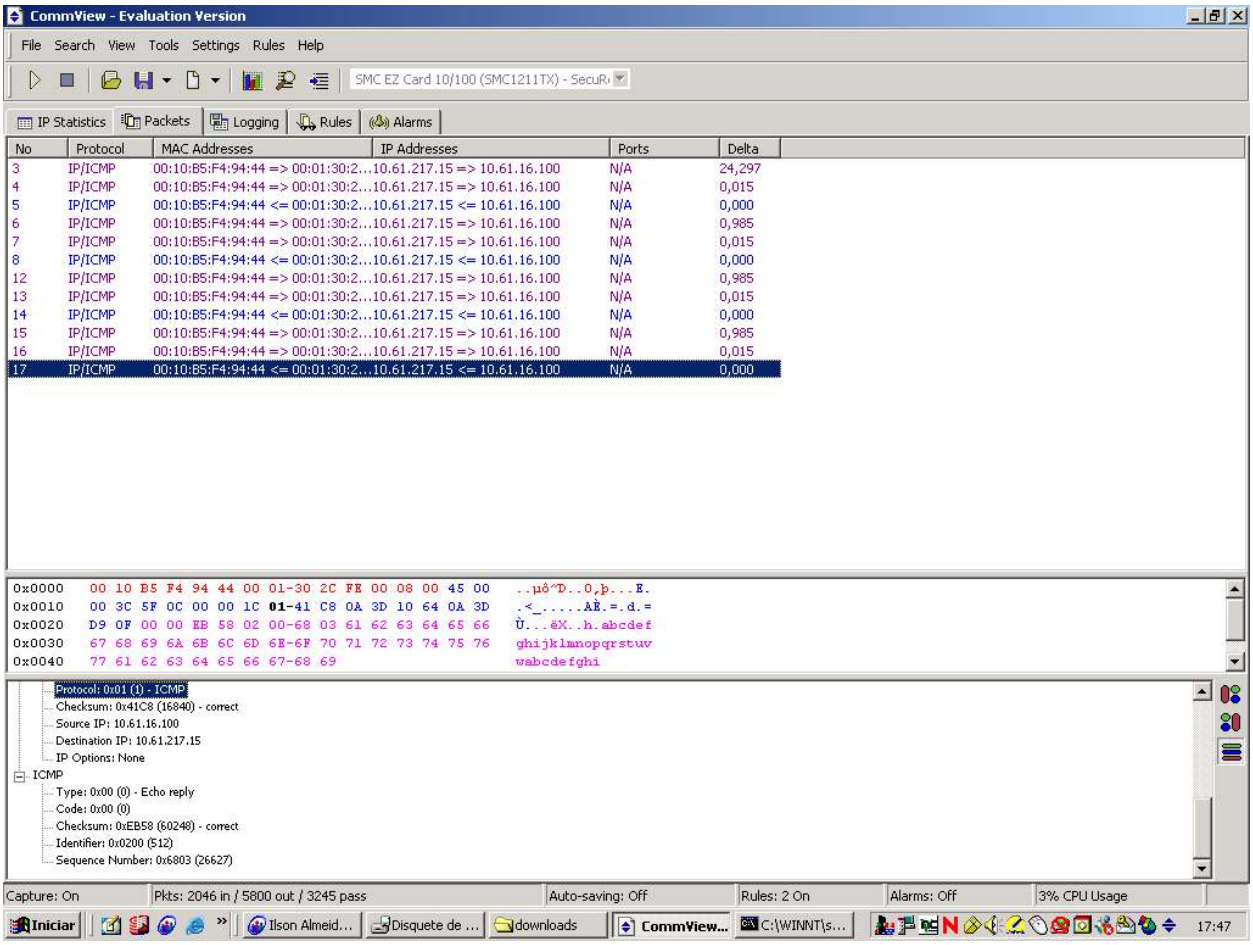
Anexo 4 sintaxe do comando tracert



Anexo 5 Configuração do connview.



Anexo 5 connview ping.



Anexo 6 connview tracert