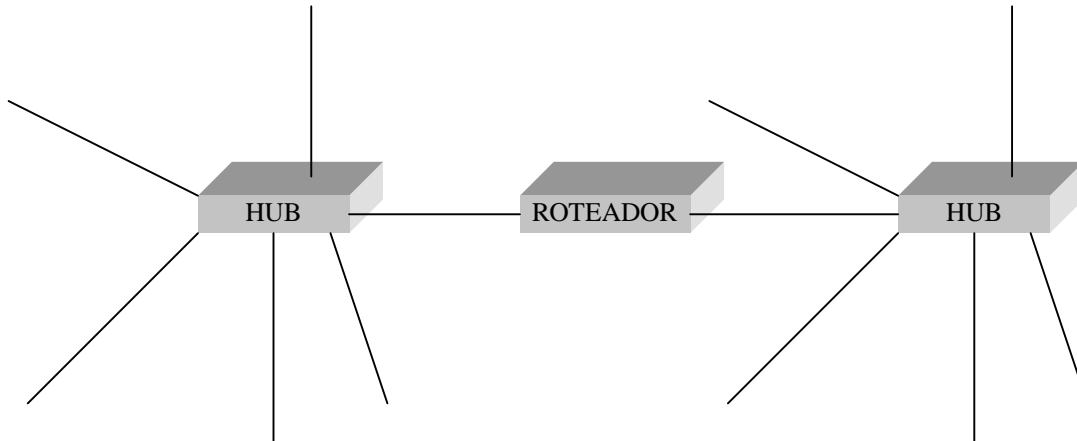


1. Alguns protocolos básicos da pilha TCP/IP

1.1 Exemplo de subredes



1.2 ICMP - Internet Control Message Protocol

ICMP é um protocolo que roda sobre IP e é usado para comunicar diversas informações de controle a outras estações, principalmente mensagens de erro. Algumas são listadas a seguir:

- **Destination Unreachable:** pacote não pôde ser entregue.
- **Redirect:** Esta mensagem é gerada por um gateway quando ele está sendo usado por outra estação, mas sabe que existe uma rota muito mais curta para chegar ao destino. Assim, redireciona o pacote ao gateway correto e gera uma mensagem à estação origem avisando da melhor rota.
- **Echo Request e Echo Reply:** Utilizado principalmente para saber se uma máquina está “viva”. Ao receber essa mensagem, a estação envia uma mensagem de Echo Reply de volta à origem. Esse recurso é usado pelo aplicativo ping e traceroute.

Outras mensagens ICMP, como as *Subnet Mask Request* e *Subnet Mask Reply* são semelhantes às *Echo Request* e *Echo Reply*, exceto que elas fornecem informações adicionais sobre a subrede à que pertence a máquina requerida.

1.3 ARP: Address Resolution Protocol

O protocolo de resolução de endereços ARP (Address Resolution Protocol) é utilizado para o mapeamento do endereço IP em números MAC. Quando inicializadas, as estações não possuem uma tabela de endereços IP<->físico armazenada. Em vez disso, para cada endereço IP solicitado que não esteja na tabela da estação, o protocolo ARP manda um pedido via broadcast de nível 2 para o endereço IP determinado. O destinatário que tiver tal endereço IP responde à máquina solicitante seu endereço físico. Nessa ocasião, tanto a



tabela da máquina origem quanto a da máquina destinatária são atualizadas com os endereços. O endereço de hardware e o endereço IP do computador então é armazenado no cache do ARP para uso futuro. Para ver a cache, pode-se utilizar o comando `arp -a`, como mostra a figura.

```
C:\> arp -a

Interface: 10.16.169.9 on Interface 0x1000002
  Endereço Internet          Endereço físico      Tipo
  10.16.169.1                02-a0-c9-d0-d9-dc   dinâmico
  10.16.169.10               00-60-97-74-02-b9   dinâmico
  10.16.169.13               00-50-04-05-8a-88   dinâmico
```

A duração da tabela de arp quando não usada é aproximadamente 2 minutos. Quando usada é de aproximadamente 10 minutos, e quando configurada estaticamente não é retirada (TCP/IP implementation details - Technet).

1.4 RARP: Reverse Address Resolution Protocol

Serve para que uma estação descubra o endereço IP associado a um endereço Ethernet. Ele é necessário, por exemplo, quando uma estação *diskless* é inicializada e necessita descobrir qual o endereço de seu servidor, por exemplo. Para obter tal informação, ela envia uma mensagem *broadcast* solicitando a algum servidor enviar seu endereço IP. Uma estação *diskless*, como se sabe, conhece seu endereço Ethernet e pouca coisa mais.

1.5 Ping

O utilitário ping envia uma seqüência de pacotes ICMP do tipo *Echo Request* para determinada localidade. O *host* que recebe essa mensagem deve enviar de volta pacotes do tipo *Echo Reply*, permitindo assim descobrir se o *host* destino está funcionando ou não, como mostra o exemplo abaixo.

```
roesler@polaris 2 % ping cs.colorado.edu
cs.colorado.edu is alive
```

Como pode-se ver, a resposta indica apenas que a máquina **cs.colorado.edu** está "viva", o que é bastante importante em determinadas situações, como por exemplo quando a comunicação não está funcionando e deseja-se saber onde está o problema.

Outra utilidade do ping é quando usa-se também a *flag -s*, que faz com que seja informado também o tempo total que a mensagem levou para ir até o destino e retornar, permitindo assim analisar o retardo da rede, e também a melhor alternativa na hora de instalar um servidor remoto. Um exemplo de utilização do **ping -s** é mostrado a seguir.

```
roesler@polaris 15 % ping -s archie.ans.net 300 20
PING forum.ans.net: 300 data bytes
308 bytes from forum.ans.net (147.225.1.10): icmp_seq=0. time=1046. ms
308 bytes from forum.ans.net (147.225.1.10): icmp_seq=1. time=904. ms
...
```



```
308 bytes from forum.ans.net (147.225.1.10): icmp_seq=18. time=932. ms
308 bytes from forum.ans.net (147.225.1.10): icmp_seq=19. time=1226. ms
```

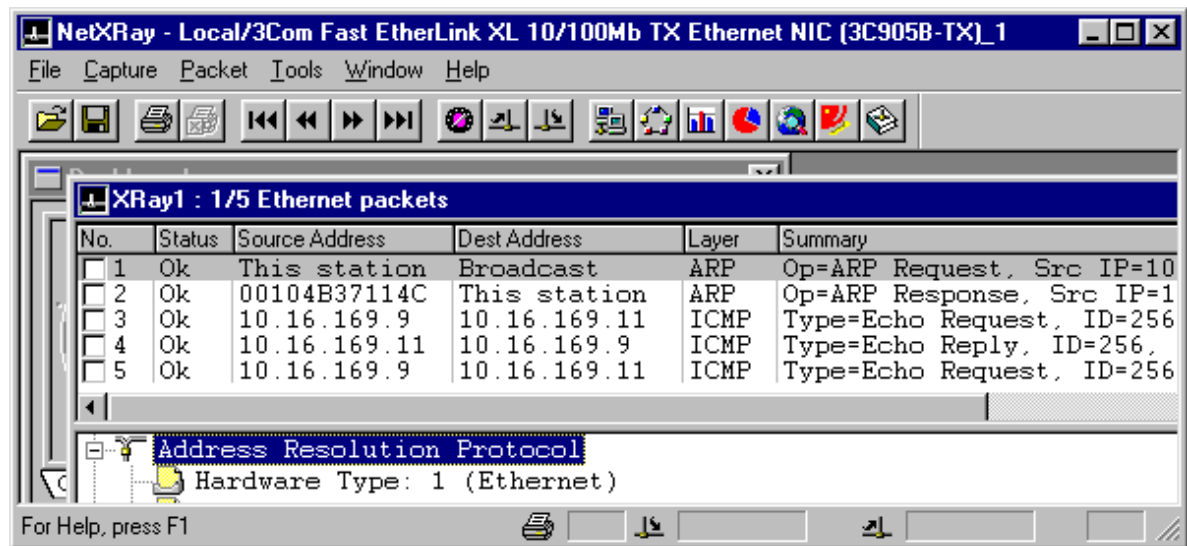
----forum.ans.net PING Statistics----

```
20 packets transmitted, 20 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 866/976/1291
```

No comando acima, ordenou-se que a mensagem de teste de eco contenha 300 bytes de dados e que seja repetida 20 vezes. A estatística mostra que as mensagens demoraram uma média de 976 ms para executar o trajeto de ida e volta ao *host* **archie.ans.net**, localizado em Nova Iorque.

Através deste utilitário, após testes com todos os *hosts* servidores possíveis e em diferentes horários, pode-se escolher o servidor que tem a rota mais rápida, para então instalar um determinado cliente (Archie, por exemplo) direcionado a ele.

A figura a seguir mostra o que acontece na rede quando se faz um ping.



1.6 Traceroute

O utilitário **traceroute**, de Van Jacobsen, envia a mensagem *Echo Request* do ICMP para determinada localidade, mas seqüencialmente incrementa o valor da variável *Time To Live* (TTL) a partir de 1. Isso faz com que o pacote retorne ao *host* origem com a variável "TTL Expired" ativada por cada *host* até onde a mensagem chega com cada TTL incrementalmente definido, até o destino final. Dessa forma, o *host* origem pode descobrir a rota feita pelas mensagens através da rede. Esse mecanismo permite determinar a estrutura da rede e é bastante padrão, não exigindo privilégios especiais para ser executado por um determinado *host*. O exemplo abaixo foi executado na estação **caracol** do Instituto de Informática da UFRGS, no dia 27 de julho de 1993, às 22:30, e mostra o caminho que percorre uma mensagem até chegar ao Japão.



```
caracol-gw% traceroute ftp.tohoku.ac.jp
traceroute to akiu.gw.tohoku.ac.jp (130.34.8.9), 30 hops max, 40 byte packets
 1 routcv (143.54.2.98) 16 ms 14 ms 15 ms
 2 routcc (143.54.1.10) 144 ms 193 ms 194 ms
 3 vortex (143.54.1.7) 82 ms 13 ms 16 ms
 4 cisco-poa (143.54.1.9) 21 ms 19 ms 18 ms
 5 cisco-sao (192.111.229.9) 42 ms 47 ms 43 ms
 6 fnal-brazil.es.net (192.74.212.5) 2195 ms 2023 ms 1714 ms
 7 fnal-e-fnal2.es.net (134.55.12.129) 2194 ms 1842 ms 2364 ms
 8 lbl-fnal.es.net (134.55.4.129) 2596 ms 2138 ms 2693 ms
 9 lbl-lc2-1.es.net (134.55.12.98) 3002 ms * 832 ms
10 llnl-lbl-t3.es.net (134.55.12.65) 735 ms 874 ms 756 ms
11 llnl-e-llnl2.es.net (134.55.12.225) 1457 ms 1515 ms 947 ms
12 ames-llnl.es.net (134.55.4.161) 1496 ms 2106 ms 2415 ms
13 ARC2.NSN.NASA.GOV (192.52.195.11) 2879 ms 1988 ms 1900 ms
14 ARC5.NSN.NASA.GOV (192.100.12.5) 1875 ms 20684 1235 ms
15 132.160.251.2 (132.160.251.2) 2322 ms 1970 ms 2498 ms
16 jp-gate.wide.ad.jp (133.4.1.1) 3061 ms 2779 ms 2815 ms
17 wnoc-snd.wide.ad.jp (133.4.4.2) 2477 ms 2460 ms 2419 ms
18 nogu.gw.tohoku.ac.jp (130.34.10.10) 2774 ms 2126 ms 2963 ms
19 izumi.gw.tohoku.ac.jp (130.34.10.3) 2448 ms 3465 ms 2740 ms
20 akiu.gw.tohoku.ac.jp (130.34.8.9) 1990 ms 1073 ms 1530 ms
```

Como pode-se notar, este utilitário é bastante importante para descobrir a topologia de uma determinada rede. Pode-se descobrir inclusive problemas de roteamento, como mostra o exemplo acima, onde a mensagem sai do roteador routcv (campus do vale, em Viamão), vai para o routcc (campus central, na reitoria, Porto Alegre), sendo então redirecionada para o vortex (campus da saúde, na rua Ramiro Barcelos), voltando em seguida para o roteador cisco-poa (na reitoria novamente), para então seguir seu caminho até o cisco-sao (São Paulo) e então seguir viagem para o exterior (Chicago, etc...). Como ficou mostrado, a mensagem faz um vai e volta da reitoria para o campus da saúde, podendo simplesmente entrar diretamente do routcc para o cisco-poa, eliminando um hop. Esse problema aconteceu devido a uma modificação de roteadores, e foi temporário.

Além disso, pode-se constatar que o maior gargalo existente na comunicação é quando a mensagem sai do Brasil (cisco-sao) e chega em Chicago (fnal-brazil-es.net). Nesse ponto ocorre um salto de tempo (de 47 ms passa para 2023 ms), mostrando que existe um congestionamento nessa rota e que há a necessidade de uma conexão mais rápida do Brasil para o exterior.



Muitas aplicações podem ser simuladas quando se sabe o protocolo e o socket correspondente. Um exemplo é usar o telnet para enviar mail, como mostra a tabela a seguir.

Comando	Argumento	Descrição
\$ telnet <ip>	25	Faz telnet na porta 25 (porta de mail)
HELO	Domínio origem	
Mail from:	Nomeorig@dominioorig	Configura originador da mensagem
RCPT to:	Nomedest@dominiodes	Configura destinatário da mensagem
Data		Avisa que é mail de dados
Subject:	Assunto	Configura assunto da mensagem
From:	Nomeorig@dominioorig	Avisa novamente originador
		Executa mensagem
.		Linha "." para finalizar mensagem
Quit		Sai do telnet

Ou para recebendo mail, utilizando telnet para a porta 110 (POP3). Comandos disponíveis:

- USER - login as a user
- PASS - specify a password
- APOP - perform secure login
- STAT - show mailbox statistics
- RETR - send a message
- LIST - show message numbers and sizes
- DELE - delete a message
- RSET - 'undo' all mailbox changes
- TOP - show lines from a message
- QUIT - close the connection



NOOP, RPOP, LAST are also supported.

Comando	Argumento	Descrição
\$ telnet <ip>	110	Faz telnet na porta 110 (porta de mail)
User	.roesler.pascal.centro6.unisinos	Configura usuário
Pass	*****	A senha ecoa na tela
List		Mostra mensagens

1.8 FTP - File Transfer Protocol

O FTP (*File Transfer Protocol*) é um método bastante comum de transferir arquivos através de redes de computadores, pois permite a entrada de um usuário em qualquer máquina que implemente este serviço (localmente ou no mundo inteiro), mesmo que o usuário não possua senha naquela máquina (*anonymous ftp*).

Para permitir este acesso, a máquina que disponibiliza seu banco de dados deve tomar certas precauções para evitar danos e acessos indevidos, assim, os diretórios e arquivos normalmente são bloqueados para escrita, e somente um certo número de comandos são disponibilizados para os usuários, como será visto adiante.

Para criar a conexão com a máquina remota, o usuário deve digitar: **ftp local.domínio**, onde **local.domínio** é o endereço da máquina que ele deseja acessar. Quando a conexão for aberta, será solicitado o nome do usuário, e ele pode digitar seu nome (caso tenha senha na máquina) ou *anonymous* (em servidores disponíveis para todos). Será solicitado então uma senha, e nesta senha é sugerido que se coloque o endereço de correio eletrônico da pessoa (**nome@local.domínio**).

Neste instante a máquina libera o usuário para acessar seu banco de dados. Os principais comandos que estão disponíveis são os seguintes:

- dir** - lista o conteúdo do diretório da máquina remota;
- cd** - troca o diretório corrente;
- bin** - busca arquivo em modo binário (necessário para arquivos comprimidos);
- get** - transfere arquivo remoto para máquina local;
- mput e mget** – transferência de múltiplos arquivos
- ...

Existem vários outros comandos, que podem ser obtidos a partir do próprio programa, que normalmente possui um *help on-line* associado.

Vale lembrar que no FTP, no POP3 e no telnet a senha vai aberta, portanto, cuidado no usar.