Pontifícia Universidade Católica de Minas Gerais
Instituto de Ciências Exatas e Informática
Departamento de Ciência da Computação
Curso de Ciência da Computação

Laboratório de Redes e Sistemas Operacionais

Comandos de Redes

Objetivos: Conhecer e verificar o funcionamento dos comandos básicos de redes de computadores via linha de comando.

Utilitários de Rede

No Windows existem alguns utilitários que usam a linha de comando e são baseados em programas originados do UNIX, com a mesma função. Os utilitários mostrados são idênticos aos do Unix com as exceções do traceroute (que no windows tem o nome de tracert devido a limitação antiga de 8 caracteres para nomes de programas do DOS) e o comando ipconfig (que no Unix/Linux é ifconfig).

1. Ping
2. Traceroute
3. Pathping
4. Route
5. Nslookup
6. Netstat
7. Ipconfig
8. arp

1. Ping

O utilitário ping (analogia com o barulho de um sonar) serve para verificar a resposta de um host até a camada de rede. O ping envia pacotes ICMP (Internet Control Message Protocol) requisitando uma resposta do host remoto. A resposta do host normalmente é o mesmo pacote enviado. Ou seja, a máquina remota simplesmente devolve os dados que ela recebeu. O objetivo é testar o funcionamento até a camada de rede, a mesma não está fazendo nenhuma tradução nos bytes enviados.

Este utilitário também verifica se a pilha de protocolos de seu computador está funcionando corretamente para tanto dê um ping no endereço 127.0.0.1 que é reservado para endereçar sua própria máquina, ou seja, um loop local (interface de loopback)

A sintaxe básica do ping é (gerada pelo próprio ping):

```
Uso: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] | [-k host-list]]
           [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
Opções:
    -t             Dispara contra o host especificado até ser interrompido.
                   Para ver as estatísticas e continuar, pressione
                   Control-Break; para parar, pressione Control-C.
    -a             Resolve endereços para nomes de host.
    -n count       Número de requisições de eco a serem enviadas.
    -l size        Envia o tamanho do buffer.
    -f             Ativa o sinalizador Don't Fragment (Não Fragmentar)  no
                   pacote (somente IPv4).
    -i TTL         Vida útil.
    -v TOS         Tipo de serviço (somente IPv4. Essa configuração foi
                   substituída e não entra em vigor no campo de tipo de
                   serviço no Cabeçalho IP).
    -r count       Grava a rota dos saltos de contagem (somente IPv4).
    -s count       Carimbo de data/hora para saltos de contagem (somente
                   IPv4).
    -j host-list   Rota ampliada de origens com lista de hosts (somente IPv4).
    -k host-list   Rota restrita de origens definida na lista de hosts
                   (somente IPv4).
    -w timeout     Tempo limite em milissegundos a aguardar para cada
                   resposta.
    -R             Usa cabeçalho de roteamento para testar também a rota
                   (somente IPv6).
    -S srcaddr     Endereço de origem a ser usado.
    -4             Força o uso do IPv4.
    -6             Força o uso do IPv6.
```

Essa sintaxe varia um pouco para o Unix. Experimente executar o ping apontando-o para um endereço conhecido. Tente pingar a máquina servidora de WWW da SBC (www.sbc.org). Veja abaixo um exemplo da saída de um ping para este endereço:

```
Disparando www.sbc.org [66.199.16.139] com 32 bytes de dados:

Resposta de 66.199.16.139: bytes=32 tempo=161ms TTL=113
Resposta de 66.199.16.139: bytes=32 tempo=171ms TTL=113
Resposta de 66.199.16.139: bytes=32 tempo=163ms TTL=113
Resposta de 66.199.16.139: bytes=32 tempo=172ms TTL=113
```

```
Estatísticas do Ping para 66.199.16.139:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 161ms, Máximo = 172ms, Média = 166ms
```

O ping mostra uma série de informações interessantes, como por exemplo, o endereço IP de destino, a quantidade de bytes enviados, o tempo de resposta de cada pacote e o TTL (*Time To Live* ou Tempo de Vida) do pacote. O ping default do Windows sempre manda 4 pacotes, no Unix, ao contrário o ping funciona indefinidamente até o usuário cancelar com control-C, esta função é feita pela opção -t no Windows.

O (TTL) *Time To Live* é um campo do pacote IP e é utilizado para limitar o número de roteadores por onde um determinado pacote pode passar. Cada roteador por onde um determinado pacote IP trafega decrementa o número do campo TTL antes de passá-lo para frente. Se o valor do campo TTL chegar a zero, o roteador não envia mais o pacote IP, e sim um outro pacote ICMP para a origem avisando que o pacote IP original teve o seu TTL=0 e por isso não pôde ser mais transmitido.

Esse mecanismo serve para evitar que em uma rede mal configurada e com algum loop de endereçamento, a quantidade de pacotes trafegada estoure a capacidade da rede por causa de retransmissões entre os mesmos roteadores. Por exemplo, se do ponto A os pacotes IP são roteados para o ponto B, e do ponto B (por causa de um erro) são roteados de volta para o ponto A, um pacote IP poderia ficar indo e voltando indefinidamente se não possuísse o mecanismo do TTL.

No caso de um endereço não responder aos pacotes enviados, isto não indica necessariamente que o computador consultado está fora do ar. Pode ter sido configurado um filtro que impeça que a máquina responda, por exemplo, o endereço www.pucminas.br

Atividade 1.

Use o comando ping para “pingar” os diversos servidores abaixo e anote os tempos máximos, mínimos e médios de resposta de cada site:

- **UAI:** www.uai.com
- **Museu do Louvre:** www.louvre.fr
- **Nintendo:** www.nintendo.co.jp

2. Traceroute

O utilitário traceroute serve para nos mostrar por onde um pacote IP trafega quando é enviado. Esse utilitário é tão útil quanto o **ping** e no Windows está disponível com o nome de **tracert**, com seu resultado um administrador de rede pode verificar em qual ponto uma comunicação pode estar rompida ou com tráfego congestionado.

A sintaxe do **tracert** no windows é:

```
Uso: tracert [-d] [-h nmax_saltos] [-j lst_hosts] [-w tempo_limite]
             [-R] [-S srcaddr] [-4] [-6] 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
                        (só IPv4).
    -w tempo_limite     Tempo de espera em milissegundos para cada resposta.
    -R                  Traça caminho de transmissão e retransmissão (só IPv6).
    -S srcaddr          Endereço de origem para uso só (IPv6).
    -4                  Força usando IPv4.
    -6                  Força usando IPv6.
```

Não existe nenhum mecanismo disponível nos roteadores para informar o trajeto de um pacote IP pela Internet. Mas sem usar nenhum artifício adicional, o autor do traceroute conseguiu fazer este programa muito bem bolado. Ele aproveitou o campo TTL do pacote IP para transmitir pacotes com TTL a partir de 1 até alcançar o destino. Assim, cada vez que um pacote "morre" no caminho até o destino, o traceroute é avisado e assim consegue traçar a rota.

Veja um exemplo de saída de um traceroute para o endereço **www.sdsc.edu**:

```
C:\WINDOWS>tracert www.sdsc.edu
Rastreando a rota para www.sdsc.edu [198.202.75.101] com no máximo 30 saltos:
  1   <10 ms   <10 ms   <10 ms  tebas.i2.com.br [200.238.196.62]
  2     2 ms     2 ms     1 ms  hardwick.i2.com.br [200.238.196.97]
  3   194 ms   148 ms   210 ms  i2-gw.pop-mg.rnp.br [200.17.183.49]
  4   473 ms   561 ms   666 ms  arrozdoce.pop-mg.com.br [200.236.165.199]
  5   416 ms     *      156 ms  casadinho-a3.pop-mg.rnp.br [200.17.183.209]
  6   234 ms   198 ms   362 ms  bb2.pop-mg.rnp.br [200.131.1.1]
  7  1080 ms  1093 ms   939 ms  border1-serial2-2.NewYork.cw.net [204.70.44.101]
  8  1032 ms  1167 ms  1161 ms  core1-fddi-0.NewYork.cw.net [204.70.2.17]
  9  1914 ms  2432 ms  2190 ms  core1-hssi-3.WestOrange.cw.net [204.70.10.14]
 10  1342 ms  1198 ms   891 ms  204.70.10.145
 11   872 ms   857 ms   932 ms  atm5-0-1.nyc-bb9.cerf.net [134.24.32.161]
 12   700 ms     *      985 ms  pos3-0-622M.nyc-bb8.cerf.net [134.24.33.158]
 13   601 ms   619 ms   850 ms  pos5-0-622M.chi-bb4.cerf.net [134.24.32.213]
 14  1040 ms   964 ms   912 ms  so4-0-0-622M.dfw-bb2.cerf.net [134.24.46.81]
 15  1057 ms  1148 ms  1287 ms  pos2-0-622M.lax-bb4.cerf.net [134.24.29.77]
 16   683 ms   673 ms   687 ms  atm1-0-2-622M.san-bb6.cerf.net [134.24.32.61]
 17     *      630 ms   656 ms  pos10-0-0-155M.san-bb1.cerf.net [134.24.29.129]
 18   655 ms   628 ms   633 ms  sdsc-gw.san-bb1.cerf.net [134.24.12.26]
 19   666 ms   708 ms   643 ms  medusa-atm.sdsc.edu [192.12.207.10]
 20   770 ms   631 ms   690 ms  www.sdsc.edu [198.202.75.101]

Rastreamento completo.
```

A saída do traceroute indica para cada *HOP* (ponto de roteamento do pacote IP), o tempo de três pacotes enviados e o endereço do roteador correspondente. Montando a sequência de 1 até o final, podemos ver por onde o pacote IP foi roteado até o destino.

O traceroute funciona enviando sucessivos pacotes IP de ping com o valor do TTL iniciando em 1 e aumentando até o ping ser respondido pelo destino. Isso faz com que o pacote IP "morra" cada vez mais longe da origem. Para cada vez que o TTL chega a zero (o pacote "morre"), o roteador onde isso ocorreu envia um pacote ICMP para a origem. Desta forma a origem tem como saber qual é o endereço do roteador onde o pacote IP morreu e consequentemente a rota dele até o destino!

Veja abaixo um exemplo de saída de traceroute em uma rede mal configurada ou com problemas de rota. Os pacotes ficam trafegando entre os IPs 200.192.56.163 e 200.192.56.161. O traceroute tem um limite de 30 rotas por default. Se qualquer rota ultrapassar este limite, o programa termina, mas isso pode ser alterado.

```
traceroute to 200.190.226.221 (200.190.226.221), 30 hops max, 40 byte packets
 1  ithaca.i2.com.br (200.238.196.17)  0.892 ms  0.88 ms  0.836 ms
 2  i2-gw.pop-mg.rnp.br (200.17.183.49)  9.694 ms  9.805 ms  72.695 ms
 3  arrozdoce.pop-mg.com.br (200.236.165.199)  47.173 ms  57.568 ms  9.666 ms
 4  casadinho-a3.pop-mg.rnp.br (200.17.183.209)  35.299 ms  29.25 ms  14.784 ms
 5  pop-mg-rnp-br-S3-7-acc01.bhe.embratel.net.br (200.251.254.73)  30.479 ms  47.494 ms
32.554 ms
 6  ebt-F5-0-dist01.bhe.embratel.net.br (200.255.153.66)  46.537 ms  47.471 ms  48.432
ms
 7  netstream-S3-0-dist01.bhe.embratel.net.br (200.251.12.50)  1201.36 ms  226.436 ms
netstream-S3-1-dist01.bhe.embratel.net.br (200.251.12.54)  293.001 ms
 8  200.192.56.163 (200.192.56.163)  294.807 ms  1316.43 ms  171.37 ms
 9  200.192.56.161 (200.192.56.161)  157.437 ms  66.189 ms  82.82 ms
10  200.192.56.163 (200.192.56.163)  1263.75 ms  879.158 ms  180.572 ms
11  200.192.56.161 (200.192.56.161)  147.899 ms  80.226 ms  148.109 ms
12  200.192.56.163 (200.192.56.163)  190.791 ms  1760.4 ms  152.392 ms
13  200.192.56.161 (200.192.56.161)  97.871 ms  130.071 ms  216.73 ms
14  200.192.56.163 (200.192.56.163)  193.109 ms  109.728 ms  132.562 ms
15  200.192.56.161 (200.192.56.161)  119.146 ms  132.605 ms  104.369 ms
16  200.192.56.163 (200.192.56.163)  239.958 ms  139.003 ms  125.818 ms
17  200.192.56.161 (200.192.56.161)  77.857 ms  107.275 ms  163.703 ms
18  200.192.56.163 (200.192.56.163)  170.308 ms  96.406 ms  90.269 ms
19  200.192.56.161 (200.192.56.161)  154.676 ms  61.096 ms  179.464 ms
20  200.192.56.163 (200.192.56.163)  196.048 ms  150.234 ms  144.485 ms
21  200.192.56.161 (200.192.56.161)  111.255 ms  75.791 ms  108.033 ms
22  200.192.56.163 (200.192.56.163)  98.99 ms  294.196 ms  298.766 ms
23  200.192.56.161 (200.192.56.161)  148.568 ms  147.442 ms  119.248 ms
24  200.192.56.163 (200.192.56.163)  233.132 ms  232.526 ms  213.243 ms
25  200.192.56.161 (200.192.56.161)  101.576 ms  101.769 ms  147.615 ms
26  200.192.56.163 (200.192.56.163)  148.876 ms  189.746 ms  259.251 ms
27  200.192.56.161 (200.192.56.161)  74.61 ms  130.222 ms  1652.72 ms
28  200.192.56.163 (200.192.56.163)  233.248 ms  161.242 ms  146.573 ms
29  200.192.56.161 (200.192.56.161)  143.745 ms  131.513 ms  122.557 ms
30  200.192.56.163 (200.192.56.163)  144.07 ms  165.208 ms  182.307 ms
```

Atividade 2.

Execute traceroute para cada um dos endereços abaixo e tente descobrir os estados ou países por onde o pacote passa.

- **UAI:** www.uai.com
- **Prefeitura de Rio Branco:** www.pmrb.ac.gov.br
- **Prefeitura de Manaus**: www.pmm.am.gov.br
- **Museu do Louvre:** www.louvre.fr
- **Nintendo:** www.nintendo.co.jp

3. Pathping

O comando **pathping** é uma ferramenta de rastreamento de rota que combina recursos dos comandos **ping** e **tracert** com informações adicionais que essas duas ferramentas não fornecem. O comando **pathping** envia pacotes para cada roteador no caminho até o destino final durante um período de tempo e depois calcula os resultados com base nos pacotes retornados de cada salto. Como o comando indica o grau de perda de pacotes em um determinado roteador ou link, fica fácil determinar quais roteadores ou links podem estar provocando problemas na rede. Há diversas opções disponíveis, como mostra a tabela a seguir.

```
Opção Nome Função
-n    Nomes de host          Não resolve endereços para nomes de host.
-h    Máximo de saltos       Especifica número máximo de saltos a pesquisar até o
destino.
-g    Lista de hosts         Caminho de origem indefinido ao longo da lista de hosts.
-p    Período                Número de milissegundos de espera entre pings.
-q    Número de consultas    Número de consultas por salto
-w    Tempo limite           Número de milissegundos a aguardar para cada resposta.
-i    endereço               Use o endereço de origem especificado.
-4    IPv4                   Força o pathping a usar IPv4.
-6    IPv6                   Força o pathping a usar IPv6.
```

O número padrão de saltos é 30, e o tempo padrão de espera antes do tempo limite é de 3 segundos. O período padrão é de 250 milissegundos, e o número padrão de consultas a cada roteador ao longo do caminho é 100.

A seguir temos um relatório típico de **pathping**. As estatísticas completas que após a lista de saltos indicam a perda de pacotes em cada roteador individual.

```
D:\>pathping -n server1

Rota de rastreamento para [10.54.1.196] acima do máximo de 30 saltos: 0  172.16.87.35 1
172.16.87.218 2  192.168.52.1 3  192.168.80.1 4  10.54.247.14 5  10.54.1.196

Computando estatísticas por 125 segundos... Origem até aqui   Este nó/link Salto  RTT
Perd./Env.= Pct  Perd./Env. = Pct  Endereço 0
172.16.87.35   0/ 100 =  0%   | 1   41ms     0/ 100 =  0%     0/ 100 =  0%
172.16.87.218 13/ 100 = 13%   | 2   22ms    16/ 100 = 16%     3/ 100 =  3%
192.168.52.1   0/ 100 =  0%   | 3   24ms    13/ 100 = 13%     0/ 100 =  0%
192.168.80.1   0/ 100 =  0%   | 4   21ms    14/ 100 = 14%     1/ 100 =  1%
10.54.247.14   0/ 100 =  0%   | 5   24ms    13/ 100 = 13%     0/ 100 =  0%
10.54.1.196

Rastreamento concluído.
```

Quando **pathping** é executado, você primeiro vê os resultados para uma rota enquanto ela é testada para verificar se tem problemas. Esse é o mesmo caminho mostrado pelo comando **tracert**. O comando **pathping** então exibe uma mensagem de ocupado durante os próximos 125 segundos (esse tempo varia de acordo com a contagem de saltos). Durante esse tempo, o **pathping** reúne informações de todos os roteadores anteriormente listados e dos links entre eles. No final desse período, exibe os resultados do teste.

As duas colunas mais à direita--**Este nó/link Perd./Env.=Pct** e **Endereço**--contêm as informações mais úteis. O link entre 172.16.87.218 (salto 1) e 192.68.52.1 (salto 2) está perdendo 13 por cento dos pacotes. Todos os outros links estão funcionando normalmente. Os roteadores nos saltos 2 e 4 também perdem pacotes endereçados a eles (como mostrado na coluna **Este nó/Vínculo**), mas essa perda não afeta seu caminho de encaminhamento.

As taxas de perda exibidas para os links (marcadas como um **|** na coluna mais à direita) indicam perdas de pacotes sendo encaminhados ao longo do caminho. Essa perda indica congestionamento no link. As taxas de perda exibidas para os roteadores (indicadas por seus endereços IP na coluna mais à direita) indicam aqueles roteadores cujas CPUs devem estar sobrecarregadas. Esses roteadores congestionados também podem ser um fator de problemas ponto a ponto, especialmente se os pacotes forem encaminhados por roteadores de software.

Atividade 3.

Execute o comando pathping no roteador acadêmico de sua unidade e anote os resultados.

Comandos relacionados:

Teste o WinMtr (Windows) ou o mtr (Linux) para acompanhar fluxos contínuos de ping para os roteadores ao longo de um caminho. Estes comandos facilitam a descoberta de enlaces com perdas ou maior atraso de comunicação.

Existem alguns aplicativos que apresentam, dentro do globo, por onde seu pacote está passando, exemplos são o Visual Route e o 3D Tracerute.

4. Route

O utilitário route é usado para listar, adicionar e remover regras da tabela de roteamento de um computador. Esta tabela de roteamento é sempre consultada pela camada de rede do protocolo para determinar qual será o próximo HOP por onde um pacote deve passar.

Usando as informações da coluna "Network Destination" e "Netmask" o computador descobre em qual regra o destino do pacote se enquadra. Identificada a regra o pacote é direcionado para o "Gateway" respectivo por uma "Interface" específica.

A primeira regra da tabela exemplo apresentada indica a regra do "Default Gateway" esta regra é a que determina para onde um pacote vai quando ele não se enquadra em nenhuma outra regra, em nosso caso, este pacote está sendo direcionado para o computador 192.168.0.1 pela interface 192.168.0.198 que é o ip local da placa de rede do computador exemplo.

Temos ainda uma regra para o endereço de loopback (127.0.0.1), outra para a própria rede que o computador participa (192.168.0.0) e outras regras usadas para broadcast e multicast.

A coluna de métrica indica qual é o custo para se alcançar o destino, sendo de grande utilidade quando um destino pode ser alcançado por dois caminhos distintos.

Atividade 4

Descubra qual é o "Default Gateway" de seu computador, observe que todo tracert que você executa o primeiro salto é feito exatamente neste gateway.

5. Nslookup

O utilitário nslookup serve para traduzir nomes de domínio para os números IP correspondentes. Este utilitário consulta os servidores de DNS (Domain Name Service) espalhados na Internet para resolver uma consulta e descobrir o endereço. Além de descobrir a tradução de nome para ip, este aplicativo pode consultar também outros tipos de registros que serão estudados quando falarmos mais detalhadamente sobre DNS.

O nslookup ao contrário dos outros utilitários vistos até agora, oferece um prompt para o usuário digitar nomes de domínios para consulta. Veja abaixo um exemplo de execução do nslookup:

```
atlanta:/home/i2/rora-> nslookup
Default Server:  i2.com.br
Address:  200.238.196.1

> www.pucmg.br.
Server:  i2.com.br
Address:  200.238.196.1

Non-authoritative answer:
Name:    www.pucminas.br
Address:  200.236.177.1
Aliases:  www.pucmg.br

> set type=mx
> flag.com.br.
Server:  i2.com.br
Address:  200.238.196.1

Non-authoritative answer:
flag.com.br     preference = 10, mail exchanger = flagnt03.flag.com.br

Authoritative answers can be found from:
flag.com.br     nameserver = flagnt03.flag.com.br
flag.com.br     nameserver = flagwall.flag.com.br
flagnt03.flag.com.br    internet address = 200.202.246.204
flagwall.flag.com.br    internet address = 200.202.246.205
> set type=a
> www.cade.com.br.
Server:  i2.com.br
Address:  200.238.196.1

Non-authoritative answer:
Name:    www.cade.com.br
Addresses:         200.244.143.187,    200.244.143.143,    200.244.143.149,
200.244.143.145
          200.244.143.148,         200.244.143.141,         200.244.143.142,
200.244.143.147, 200.244.143.1
46
          200.244.143.140
```

O que foi digitado pelo usuário está em **negrito**. Note que além dos domínios, existem alguns comandos disponíveis no nslookup (set type=). Quando os domínios são seguidos de um ponto, nslookup interpreta como domínios completos. É possível especificar somente um nome de uma máquina e o programa busca pelo seu endereço IP dentro da própria rede.

Use o comando **help** para ter acesso aos demais comandos do nslookup. Veja a saída de um help do nslookup no Unix:

```
> help
$Id: nslookup.help,v 8.4 1996/10/25 18:09:41 vixie Exp $

Commands:       (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands; see nslookup(1) for details
set OPTION      - set an option
    all         - print options, current server and host
    [no]debug   - print debugging information
    [no]d2      - print exhaustive debugging information
    [no]defname - append domain name to each query
    [no]recurse - ask for recursive answer to query
    [no]vc      - always use a virtual circuit
    domain=NAME - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME   - set root server to NAME
    retry=X     - set number of retries to X
    timeout=X   - set initial time-out interval to X seconds
    querytype=X - set query type, e.g., A, ANYÇNAME, HINFO, MX, PX, NS, PTR, SOA, TXT,
WKS, SRV, NAPTR
    port=X      - set port number to send query on
    type=X      - synonym for querytype
    class=X     - set query class to one of IN (Internet), CHAOS, HESIOD or ANY
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
finger [USER]   - finger the optional USER at the current default host
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -h          -  list HINFO (CPU type and operating system)
    -s          -  list well-known services
    -d          -  list all records
    -t TYPE     -  list records of the given type (e.g., AÇNAME,MX, etc.)
view FILE       - sort an 'ls' output file and view it with more
exit            - exit the program, ^D also exits
>
```

Atividade 5.

Descubra os endereços IP das máquinas que podem receber e-mail das seguintes empresas:

- Google
- Yahoo
- UAI
- Louvre

Acesse o registro.br, o www.nic.fr ou o whois.net e descubra as pessoas responsáveis pelos sites acima.

6. Netstat

O netstat serve para mostrar as conexões ativas atualmente com a máquina em questão. Ele lista na tela todas as conexões TCP/IP em andamento. Além disso, existe uma opção para mostrar o conteúdo da tabela de roteamento. Veja abaixo a sintaxe do netstat do windows:

```
Exibir estatísticas de protocolo e conexões de rede TCP/IP atuais.

NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]

  -a            Exibe todas as conexões e portas de escuta.
  -e            Exibe estatísticas Ethernet.  Isso pode ser combinado à
                opção -s.
  -n            Exibe endereços e números de porta em formato numérico.
  -p proto      Exibe conexões para o protocolo especificado por proto; proto
                pode ser tcp ou udp.  Se usado com a opção -s para exibir
                estatísticas por protocolo, proto pode ser tcp, udp ou ip.
  -r            Exibe o conteúdo da tabela de roteamento.
  -s            Exibe estatísticas por protocolo.  Por padrão, as estatísticas
                são mostradas para TCP, UDP e IP; a opção -p pode ser usada
                para especificar um subconjunto do padrão.
 intervalo      Exibe novamente uma estatística selecionada, fazendo pausas de
                intervalos de segundos entre cada tela.  Pressione CTRL+C para
                interromper a nova exibição das estatísticas.  Caso omitido,
                netstat imprimirá as informações de configuração uma vez.
```

Atividade 6.

Use o netstat para mostrar todas as conexões e portas de escuta da sua máquina (LISTENING). A saída é mostrada em 4 colunas. Na primeira está o protocolo, na segunda o endereço da conexão na porta local. A terceira coluna mostra o endereço na máquina remota (o endereço da máquina e a porta TCP da conexão) e a quarta coluna mostra o estado da conexão (ESTABLISHED, LISTENING, CLOSE_WAIT, etc).

Use a opção **-r** para mostrar o conteúdo da tabela de roteamento da sua estação. Essa tabela mostra para qual endereço cada pacote deve ser enviado em função do seu endereço IP. Desta forma, a máquina garante que o pacote será entregue para a máquina de destino corretamente.

7. ipconfig

No Windows existe o aplicativo IPCONFIG disponível na linha de comando do Windows e que mostra as configurações da interface de rede, para Linux o comando é IFCONFIG. Veja abaixo um exemplo de saída um IPCONFIG:

```
X:\>ipconfig /all

Configuração de IP do Windows NT
        Nome do host . . . . . . . . . . : cairo.i2.com.br
        Servidores DNS . . . . . . . . . : 200.238.196.49
                                           200.238.196.1
                                           200.131.1.51
        Tipo de nó . . . . . . . . . . . : Híbrida
        Identificador de escopo NetBIOS. :
        Roteamento de IP ativado . . . . : Não
        Proxy WINS ativado . . . . . . . : Não
        Resolução NetBIOS usa DNS. . . . : Sim

Ethernet adaptador PGPMacMP5:
        Descrição. . . . . . . . . . . . : Novell 2000 Adapter.
        Endereço físico. . . . . . . . . : 00-00-B4-9E-45-6C
        DHCP ativado . . . . . . . . . . : Não
        Endereço IP. . . . . . . . . . . : 200.238.196.50
        Máscara de sub-rede. . . . . . . : 255.255.255.224
        Gateway padrão . . . . . . . . . : 200.238.196.33
        Servidor WINS primário . . . . . : 200.238.196.49

Ethernet adaptador NdisWan4:
        Descrição. . . . . . . . . . . . : NdisWan Adapter
        Endereço físico. . . . . . . . . : 00-00-00-00-00-00
        DHCP ativado . . . . . . . . . . : Não
        Endereço IP. . . . . . . . . . . : 0.0.0.0
        Máscara de sub-rede. . . . . . . : 0.0.0.0
        Gateway padrão . . . . . . . . . :
```

Siginificados:

- **DHCP**: dinamic host configuration protocol - um protocolo de configuração automático para parâmetros de rede (IP, DNS, gateway, etc) cujo objetivo é reduzir o tempo e o trabalho para configurar um grande número de máquinas
- **DNS**: domain name service - serviço de tradução de nomes para IP disponível na Internet
- **NetBIOS**: network basic input output system - uma API para aplicações de usuários enviarem e receberem diretivas de controle de I/O de uma forma geral em uma rede local
- **WINS**: windows internet naming service - é um serviço de tradução de nomes (como o DNS) sobre NetBIOS
- **Endereço Físico (Endereço MAC)**: É o endereço Ethernet de 48 bits que cada adaptador de rede possui e que é alocado pelo fabricante da placa.

Execute o comando ipconfig /all e através das informações apresentadas faça um esboço da rede do seu laboratório.

Atividade 7.

Descubra pelo endereço MAC[1] o fabricante da placa e seu endereço de correspondência.

[1] Acesse http://standards.ieee.org/develop/regauth/oui/oui.txt, para a lista de fabricantes de adaptadores de rede Ethernet.

8. ARP

O comando ARP exibe e modifica entradas no cache do protocolo de resolução de endereços (ARP), que contém uma ou mais tabelas que são usadas para armazenar endereços IP e seus endereços físicos Ethernet ou Token Ring resolvidos. Há uma tabela separada para cada adaptador de rede Ethernet ou Token Ring instalado no computador. Quando utilizado sem parâmetros, **arp** exibe informações de ajuda.

Sintaxe

arp[**-a** [*End_IP_da_rede*] [**-N***End_da_interface*]] [**-g** [*End_IP_da_rede*] [**-N***End_da_interface*]] [**-d***End_IP_da_rede* [*End_da_interface*]] [**-s***End_IP_da_rede End_Ether* [*End_da_interface*]]

Parâmetros

-a[*End_IP_da_rede*] [-N*End_da_interface*]

Exibe as tabelas do cache ARP atual para todas as interfaces. Para exibir a entrada de cache ARP de um endereço IP específico, use **arp -a** com o parâmetro *End_IP_Da_Rede*, onde *End_IP_Da_Rede* é um endereço IP. Se *End_IP_Da_Rede* não for especificado, será utilizada a primeira interface aplicável. Para exibir a tabela de cache ARP de uma interface específica, use o parâmetro **-N***End_da_interface* em conjunto com o parâmetro **-a**, onde *End_da_interface* é o endereço IP atribuído à interface. O parâmetro **-N** diferencia maiúsculas de minúsculas.

-g[*End_IP_da_rede*] [-N*End_da_interface*]

Idêntico a **-a**.

-d*End_IP_da_rede* [*End_da_interface*]

Exclui uma entrada com um endereço IP específico, onde *End_IP_da_rede* é o endereço IP. Para excluir uma entrada de uma tabela para uma interface específica, use o parâmetro *End_da_interface* onde *End_da_interface* é o endereço IP atribuído à interface. Para excluir todas as entradas, use o caractere curinga asterisco (*) em vez de *End_IP_da_rede*.

-s*End_IP_da_rede End_Ether* [*End_da_interface*]

Adiciona uma entrada estática ao cache ARP que resolve o endereço IP *End_IP_da_rede* para o endereço físico *End_Ether*. Para adicionar uma entrada estática do cache ARP à tabela para uma interface específica, use o parâmetro *End_da_interface* onde *End_da_interface* é um endereço IP atribuído à interface.

/?

Exibe informações de ajuda no prompt de comando.

Comentários

- Os endereços IP de *End_IP_da_rede* e *End_da_interface* são expressos em notação decimal pontilhada.
- O endereço físico de *End_Ether* consiste em seis bytes expressos em notação hexadecimal e separados por hífens (por exemplo, 00-AA-00-4F-2A-9C).
- As entradas adicionadas com o parâmetro **-s** são estáticas e não atingem o tempo limite no cache ARP. As entradas serão removidas se o protocolo TCP/IP for interrompido e iniciado. Para criar entradas de cache ARP estáticas permanentes, coloque os comandos **arp** adequados em um arquivo em lotes e use Tarefas agendadas para executar esse arquivo na inicialização.

Exemplos

Para exibir as tabelas do cache ARP para todas as interfaces, digite:

arp -a

Para exibir a tabela do cache ARP para a interface a que está atribuído o endereço IP 10.0.0.99, digite:

arp -a -N 10.0.0.99

Para adicionar uma entrada estática do cache ARP que resolva o endereço IP 10.0.0.80 para o endereço físico 00-AA-00-4F-2A-9C, digite:

arp -s 10.0.0.80 00-AA-00-4F-2A-9C

Atividade 8

Através do comando ARP descubra o endereço MAC e os fabricantes das placas de rede dos servidores DNS, DHCP e o default gateway.

Atividade 9

Refaça os comandos através de ferramentas online disponíveis na internet.

Ping.eu

http://network-tools.com/

8. NET

Outro comando de prompt muito utilizado em redes locais é o NET, mas este eu deixo para vcs aprenderem sozinho.