INSTITUTO FEDERAL
Santa Catarina
Câmpus São José

Ferramentas básicas: ifconfig, ip e ping

Redes de computadores - Laboratório 01

Curso: Engenharia de Telecomunicações
Professor: Odilson Tadeu Valle

Aluno:
Victor E. de L. Guerra

22/08/2025

Sumário

1 ifconfig ou ip

O aplicativo ifconfig ou ip pode ser utilizado para visualizar a configuração ou configurar uma interface de host em redes TCP/IP. Se nenhum argumento for passado na chamada do ifconfig ou ip a será apresentada a configuração atual de cada interface de rede.

Consultar as páginas man ifconfig ou man ip do Linux para maiores detalhes sobre o funcionamento deste aplicativo, o qual permite ativar/desativar a interface, configurar o endereço IP, definir o tamanho da MTU, redefinir o endereço de hardware se a interface suporta, redefinir a interrupção utilizada pelo dispositivo, entre outros.

1.1 Quantas e quais interfaces de rede sua máquina possui? Liste.

A minha máquina atual, utilizada durante a resolução deste laboratório, possuí 3 interfaces de redes, a ***dokcer0*** a ***eth0*** e a ***lo***, conforme apresentado na imagem a seguir:

```
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 9e:0b:e1:fe:c1:be  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 191.36.13.78  netmask 255.255.255.192  broadcast 191.36.13.127
        inet6 fe80::aaa1:59ff:fe95:c9a8  prefixlen 64  scopeid 0x20<link>
        inet6 2804:1454:1004:311::1016  prefixlen 128  scopeid 0x0<global>
        ether a8:a1:59:95:c9:a8  txqueuelen 1000  (Ethernet)
        RX packets 65367  bytes 62102607 (59.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 57371  bytes 51628424 (49.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 701  bytes 43347 (42.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 701  bytes 43347 (42.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 1: Listagem das interfaces de redes da máquina

1.2 Quais são os endereços da camada 2 atribuídos às interfaces? De onde o sistema obteve esses endereços?

Como apresentado na Figura 1, podemos verificar que apenas as interfaces ***docker0*** e ***eth0*** possuem endereço de camada 2, sendo eles *9e:0b:e1:fe:c1:be* e *a8:a1:59:95:c9:a8*, respectivamente.

O endereço da camada 2 da interface ***eth0*** é atribuído pela própria placa de rede física (hardware), vindo de fábrica pelo fabricante da NIC, embora possa ser alterado manualmente pelo sistema operacional. Já o endereço da interface ***docker0*** não vem de hardware, mas é gerado pelo kernel/Docker no momento da criação da interface virtual, geralmente a partir de um endereço MAC aleatório do espaço reservado para endereços *locally administered*.

1.3 Quais são os endereços IPv4? De onde o sistema obteve esses endereços?

Como podemos visualizar na Figura 1, os endereços **IPv4** atribuídos às interfaces ***docker0***, ***eth0*** e ***lo*** são, respectivamente, *172.17.0.1*, *191.36.13.78* e *127.0.0.1*.

O endereço da interface ***eth0*** foi atribuído pela rede externa, geralmente via servidor *DHCP* do provedor de internet ou configurado manualmente. Já o endereço da interface ***docker0*** foi definido automaticamente pelo Docker no momento da criação da *bridge* virtual. Por fim, o endereço da interface ***lo*** é o endereço reservado de *loopback* (`127.0.0.1`), atribuído pelo próprio sistema operacional para permitir comunicação interna no host.

1.4 Suas interfaces tem IPv6 configurado? Qual o endereço e escopo dos mesmos?

Apenas as interfaces de rede ***eth0*** e ***lo*** tem IPv6 vinculados. A seguir, podemos verificar uma relação entre o endereço e o escopo do endereço para cada uma das máquinas:

- Interface **eth0**:
  - IPv6 escopo global: `2804:1454:1004:311::1016`
  - IPv6 escopo local: `fe80::aaa1:59ff:fe95:c9a8`
- Interface **lo**:
  - IPv6 escopo local: `::1`

1.5 Use o link 'Verificando a estrutura do endereço IP' para explorar a estrutura do seu endereço IPv4 da interface eth0. Recorte e cole no relatório.

```
Address:   191.36.13.78          10111111.00100100.00001101.01 001110
Netmask:   255.255.255.192 = 26  11111111.11111111.11111111.11 000000
Wildcard:  0.0.0.63              00000000.00000000.00000000.00 111111
=>
Network:   191.36.13.64/26       10111111.00100100.00001101.01 000000 (Class B)
Broadcast: 191.36.13.127         10111111.00100100.00001101.01 111111
HostMin:   191.36.13.65          10111111.00100100.00001101.01 000001
HostMax:   191.36.13.126         10111111.00100100.00001101.01 111110
Hosts/Net: 62
```

Figura 2: IP Calculator

2 ping

Aplicativo ping permite a um usuário verificar se um host remoto está ativo. É bastante utilizado para detectar problemas de comunicação na rede. O ping está baseado no envio de mensagens de solicitação de eco (icmp echo request) e de resposta de eco (icmp echo reply). Estas mensagens fazem parte do rol de mensagens do protocolo ICMP, que é um protocolo de reportagem de erros, a ser estudado mais tarde, componente do protocolo IP.

O ping é um dos principais comandos a disposição do administrador de rede no sentido de verificar a conectividade em rede. Por exemplo, se houver resposta de um ping a partir de um servidor remoto, significa que a máquina local está rodando corretamente o TCP/IP, o enlace local está funcionando corretamente, o roteamento entre a origem e o destino está operando, e por fim, a máquina remota também está rodando corretamente o TCP/IP.

2.1 Envie ping4 para diferentes hosts e compare os tempos de resposta:

2.1.1 No endereço local de loopback:

```
aluno: ~$ ping4 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.073 ms
```

Figura 3: Ping4 feito no endereço local de loopback

2.1.2 servidores externos:

- **ifsc.edu.br**:

```
PING ifsc.edu.br (191.36.0.94) 56(84) bytes of data.
64 bytes from 191.36.0.94 (191.36.0.94): icmp_seq=1 ttl=58 time=0.633 ms
64 bytes from 191.36.0.94 (191.36.0.94): icmp_seq=2 ttl=58 time=0.767 ms
64 bytes from 191.36.0.94 (191.36.0.94): icmp_seq=3 ttl=58 time=1.10 ms
64 bytes from 191.36.0.94 (191.36.0.94): icmp_seq=4 ttl=58 time=0.713 ms
```

Figura 4: Ping4 feito no endereço ifsc.edu.br

- **www.uol.com.br**:

```
PING  (92.123.2.38) 56(84) bytes of data.
64 bytes from a92-123-2-38.deploy.static.akamaitechnologies.com (92.123.2.38): icmp_seq=1 ttl=55 time=0.710 ms
64 bytes from a92-123-2-38.deploy.static.akamaitechnologies.com (92.123.2.38): icmp_seq=2 ttl=55 time=1.12 ms
64 bytes from a92-123-2-38.deploy.static.akamaitechnologies.com (92.123.2.38): icmp_seq=3 ttl=55 time=0.705 ms
64 bytes from a92-123-2-38.deploy.static.akamaitechnologies.com (92.123.2.38): icmp_seq=4 ttl=55 time=1.01 ms
```

Figura 5: Ping4 feito no endereço www.uol.com.br

- **www.aaa.jp**:

```
PING aaa.jp (219.94.128.109) 56(84) bytes of data.
64 bytes from www899.sakura.ne.jp (219.94.128.109): icmp_seq=1 ttl=45 time=281 ms
64 bytes from www899.sakura.ne.jp (219.94.128.109): icmp_seq=2 ttl=45 time=282 ms
64 bytes from www899.sakura.ne.jp (219.94.128.109): icmp_seq=3 ttl=45 time=281 ms
64 bytes from www899.sakura.ne.jp (219.94.128.109): icmp_seq=4 ttl=45 time=281 ms
```

Figura 6: Ping4 feito no endereço www.aaa.jp

2.1.3 Explique as diferenças entre os tempos de resposta dos ping realizados:

- **1. Entre ping para diferentes destinos:**

  Pude verificar que para destinos dentro do Brasil (.br), a latência média de resposta é menor que 1.0 ms, já quando fiz o ping para um um destino fora do Brasil (.jp) obtive uma latência de resposta muito maior (cerca de 281 ms), isso por conta do tempo de propagação fisicamente do pacote. Já comparando todos esses pings ao ping feito para o endereço local de loopback, podemos ver que o tempo de resposta é muito menor (cerca de 0.07 ms)

- **2. Entre respostas recebidas de um mesmo destino:**

  Pude perceber que, por exemplo, no ping que realizei para o endereço ifsc.edu.br, ocorreu uma certa oscilação no tempo de resposta, e isso se da por conta do congestionamento naquele determinado momento no roteador.

2.1.4 Consulte as páginas man e teste o ping com os parâmetros abaixo e descreva suas funcionalidades:

Consultando a página de manual (`man ping`) e realizando testes práticos, foi possível observar o funcionamento dos seguintes parâmetros:

- **-c *count***: define a quantidade de pacotes ICMP a serem enviados.
  - Exemplo: `ping -c 4 ifsc.edu.br` envia apenas 4 pacotes e finaliza o teste.
- **-i *interval***: define o intervalo (em segundos) entre o envio de cada pacote.
  - Exemplo: `ping -i 2 ifsc.edu.br` envia um pacote a cada 2 segundos.
- **-s *packetsize***: altera o tamanho da carga útil (payload) do pacote ICMP. O valor padrão é 56 bytes (mais 8 bytes do cabeçalho ICMP, totalizando 64 bytes).
  - Exemplo: `ping -s 200 ifsc.edu.br` envia pacotes ICMP com 200 bytes de carga útil.
- **-t *ttl***: define o valor do campo *Time To Live* no cabeçalho IP. O TTL indica o número máximo de roteadores que o pacote pode atravessar.
  - Exemplo: ao iniciar com `ping -t 1 ifsc.edu.br`, o pacote atinge apenas o primeiro roteador, retornando a mensagem de "Time Exceeded". Ao incrementar progressivamente o valor de `ttl`, é possível descobrir cada roteador intermediário no caminho até o destino. Essa é a mesma técnica utilizada pelo comando `traceroute`.

2.1.5 Tente o ping6 para outros sites:

Nesta última parte de laboratório, optei por fazer o ping6 para outros dois sites, o *ifsc.edu.br* e para o *google.com*

- *ifsc.edu.br*:

  Podemos ver que ao tentar fazer o ping6 para o endereço ifsc.edu.br ele nos retorna uma mensagem informando que a máquina não suporta essa família de endereços.

```
ping6: ifsc.edu.br: Família de endereços não suportada para nome de máquina
```

Figura 7: Ping6 feito para ifsc.edu.br

- *google.com*:

  Já ao tentar realizar o ping6 para o endereço google.com obtivemos resposta, indicando que a máquina suporta e tem configurado o IPv6.

```
PING google.com(2800:3f0:4001:809::200e (2800:3f0:4001:809::200e)) 56 data bytes
64 bytes from 2800:3f0:4001:809::200e (2800:3f0:4001:809::200e): icmp_seq=1 ttl=113 time=15.4 ms
64 bytes from 2800:3f0:4001:809::200e (2800:3f0:4001:809::200e): icmp_seq=2 ttl=113 time=15.7 ms
64 bytes from 2800:3f0:4001:809::200e (2800:3f0:4001:809::200e): icmp_seq=3 ttl=113 time=15.7 ms
64 bytes from 2800:3f0:4001:809::200e (2800:3f0:4001:809::200e): icmp_seq=4 ttl=113 time=15.4 ms
64 bytes from 2800:3f0:4001:809::200e (2800:3f0:4001:809::200e): icmp_seq=5 ttl=113 time=15.7 ms
```

Figura 8: Ping6 feito para google.com