

Validação da configuração de rede

Coleta das informações da interface de rede

O comando `ip link show` lista todas as interfaces de rede disponíveis em seu sistema.

No exemplo a seguir, o servidor tem três interfaces de rede: `lo`, que é o dispositivo de loopback que está conectado ao próprio servidor e duas interfaces de ethernet, `ens3` e `ens4`.

```
[user@host ~]$ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc m
q state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:00:00:0a brd ff:ff:ff:ff:ff:ff
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc m
q state UP mode DEFAULT group default qlen 1000
    link/ether 52:54:00:00:00:1e brd ff:ff:ff:ff:ff:ff
```

Para configurar uma interface de rede corretamente, você precisa saber qual delas está conectada a qual rede.

Muitas vezes, você pode obter um endereço MAC da interface conectada a cada rede, seja porque está fisicamente impressa na placa ou no servidor ou porque é uma máquina virtual, e você sabe como ela está configurada.

O endereço MAC do dispositivo é listado após `link/ether` para cada interface. Então você sabe que a placa de rede com o endereço MAC `52:54:00:00:00:0a` é a interface de rede `ens3`.

Exibição dos endereços IP

Use o comando `ip` para visualizar as informações do dispositivo e de endereço. Uma interface de rede única pode ter vários endereços IPv4 ou IPv6.

```
[user@host ~]$ip addr show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc p
fifo_fast state UP qlen 1000
    link/ether 52:54:00:00:00:0b brd ff:ff:ff:ff:ff:ff
    inet 192.0.2.2/24 brd 192.0.2.255 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 2001:db8:0:1:5054:ff:fe00:b/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe00:b/64 scope link
        valid_lft forever preferred_lft forever
```

- Uma interface ativa é `UP`.
- A string `link/ether` especifica o endereço (MAC) do hardware do dispositivo.
- A string `inet` mostra um endereço IPv4, a extensão de seu prefixo de rede e o escopo.
- A string `inet6` mostra um endereço IPv6, a extensão de seu prefixo de rede e o escopo. Este endereço é de escopo *global* e é usado normalmente
- A string `inet6` mostra que a interface tem um endereço IPv6 de escopo *link*, que só pode ser usado para comunicação no link de ethernet local.

Exibição de estatísticas de desempenho

O comando `ip` também pode mostrar as estatísticas sobre o desempenho da rede. Os contadores para cada interface de rede podem identificar a presença de problemas de rede.

Os contadores registram estatísticas de elementos como o número de pacotes recebidos (RX) e transmitidos (TX), erros de pacotes e pacotes que foram descartados.

```
[user@host ~]$ip -s link show ens3
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc p
```

```
fifo_fast state UP qlen 1000
link/ether 52:54:00:00:00:0a brd ff:ff:ff:ff:ff:ff
  RX: bytes  packets  errors  dropped overrun mcast
    269850    2931      0        0         0         0
  TX: bytes  packets  errors  dropped carrier collsns
    300556    3250      0        0         0         0
```

Verificação da conectividade entre hosts

O comando `ping` testa a conectividade. O comando continuará sendo executado até você pressionar **Ctrl+c**, a menos que sejam indicadas opções para limitar o número de pacotes enviados.

```
[user@host ~]$ping -c3 192.0.2.254
PING 192.0.2.1 (192.0.2.254) 56(84) bytes of data.
64 bytes from 192.0.2.254: icmp_seq=1 ttl=64 time=4.33 ms
64 bytes from 192.0.2.254: icmp_seq=2 ttl=64 time=3.48 ms
64 bytes from 192.0.2.254: icmp_seq=3 ttl=64 time=6.83 ms

--- 192.0.2.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 200
3ms
rtt min/avg/max/mdev = 3.485/4.885/6.837/1.424 ms
```

O comando `ping6` é a versão IPv6 do comando `ping` no Red Hat Enterprise Linux. A diferença entre esses comandos é que o comando `ping6` se comunica por IPv6 e recebe endereços IPv6.

```
[user@host ~]$ping6 2001:db8:0:1::1
PING 2001:db8:0:1::1(2001:db8:0:1::1) 56 data bytes
64 bytes from 2001:db8:0:1::1: icmp_seq=1 ttl=64 time=18.4
ms
64 bytes from 2001:db8:0:1::1: icmp_seq=2 ttl=64 time=0.178
ms
64 bytes from 2001:db8:0:1::1: icmp_seq=3 ttl=64 time=0.180
ms
```

```

^C
--- 2001:db8:0:1::1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 200
1ms
rtt min/avg/max/mdev = 0.178/6.272/18.458/8.616 ms
[user@host ~]$

```

Quando você faz ping dos endereços link-local e do grupo multicast link-local para todos os nós (`ff02::1`), a interface de rede a ser usada deve ser explicitamente especificada com um identificador de zona de escopo (como `ff02::1%ens3`).

Se essa interface de rede for omitida, o erro *connect: Invalid argument* será exibido.

Você pode usar o comando `ping6 ff02::1` para encontrar outros nós IPv6 na rede local.

```

[user@host ~]$ping6 ff02::1%ens4
PING ff02::1%ens4(ff02::1) 56 data bytes
64 bytes from fe80::78cf:7fff:fed2:f97b: icmp_seq=1 ttl=64
time=22.7 ms
64 bytes from fe80::f482:dbff:fe25:6a9f: icmp_seq=1 ttl=64
time=30.1 ms (DUP!)
64 bytes from fe80::78cf:7fff:fed2:f97b: icmp_seq=2 ttl=64
time=0.183 ms
64 bytes from fe80::f482:dbff:fe25:6a9f: icmp_seq=2 ttl=64
time=0.231 ms (DUP!)
^C
--- ff02::1%ens4 ping statistics ---
2 packets transmitted, 2 received, +2 duplicates, 0% packet
loss, time 1001ms
rtt min/avg/max/mdev = 0.183/13.320/30.158/13.374 ms
[user@host ~]$
[user@host ~]$ping6 -c 1 fe80::f482:dbff:fe25:6a9f%ens4
PING fe80::f482:dbff:fe25:6a9f%ens4(fe80::f482:dbff:fe25:6a
9f) 56 data bytes
64 bytes from fe80::f482:dbff:fe25:6a9f: icmp_seq=1 ttl=64

```

```
time=22.9 ms
```

```
--- fe80::f482:dbff:fe25:6a9f%ens4 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 22.903/22.903/22.903/0.000 ms
```

Os endereços link-local IPv6 podem ser usados por outros hosts no mesmo link, como endereços normais.

```
[user@host ~]$ssh fe80::f482:dbff:fe25:6a9f%ens4  
user@fe80::f482:dbff:fe25:6a9f%ens4's password:  
Last login: Thu Jun  5 15:20:10 2014 from host.example.com  
[user@server ~]$
```

Solução de problemas com roteadores

O roteamento de rede é complexo e, às vezes, o tráfego não se comporta como você espera. Você pode usar diferentes ferramentas para diagnosticar problemas de roteador.

Descrição da tabela de roteamento

Use a opção `route` do comando `ip` para mostrar as informações de roteamento.

```
[user@host ~]$ip route  
default via 192.0.2.254 dev ens3 proto static metric 1024  
192.0.2.0/24 dev ens3 proto kernel scope link src 192.0.2.2  
10.0.0.0/8 dev ens4 proto kernel scope link src 10.0.0.11
```

Todos os pacotes destinados à rede `10.0.0.0/8` são enviados diretamente para o destino pelo dispositivo `ens4`. Todos os pacotes destinados à rede `192.0.2.0/24` são enviados diretamente para o destino pelo dispositivo `ens3`. Todos os outros pacotes são enviados para o roteador padrão

em `192.0.2.254` e também pelo dispositivo `ens3`.

Use a opção `-6` do comando `ip` para mostrar a tabela de roteamento IPv6.

```
[user@host ~]$ip -6 route
unreachable ::/96 dev lo  metric 1024  error -101
unreachable ::ffff:0.0.0.0/96 dev lo  metric 1024  error -101
2001:db8:0:1::/64 dev ens3  proto kernel  metric 256
unreachable 2002:a00::/24 dev lo  metric 1024  error -101
unreachable 2002:7f00::/24 dev lo  metric 1024  error -101
unreachable 2002:a9fe::/32 dev lo  metric 1024  error -101
unreachable 2002:ac10::/28 dev lo  metric 1024  error -101
unreachable 2002:c0a8::/32 dev lo  metric 1024  error -101
unreachable 2002:e000::/19 dev lo  metric 1024  error -101
unreachable 3ffe:ffff::/32 dev lo  metric 1024  error -101
fe80::/64 dev ens3  proto kernel  metric 256
default via 2001:db8:0:1::ffff dev ens3  proto static  metric 1024
```

1. A rede

`2001:db8:0:1::/64` usa a interface `ens3` (que, presumivelmente, tem um endereço nessa rede).

2. A rede

`fe80::/64` usa a interface `ens3`, para o endereço link-local. Em um sistema com várias interfaces, existe uma rota para a rede `fe80::/64` em cada interface para cada endereço link-local.

3. A rota padrão para todas as redes na internet IPv6 (a rede

`::/0`) usa o roteador na rede `2001:db8:0:1::ffff` e é acessível com o dispositivo `ens3`.

Rastrear rotas de tráfego

Para rastrear o caminho do tráfego de rede até chegar a um host remoto por diversos roteadores, use o comando `tracert` ou `tracert`.

Esses comandos podem identificar problemas com um dos seus roteadores ou em um roteador intermediário.

Os dois comandos usam pacotes UDP para rastrear o caminho por padrão. Entretanto, muitas redes bloqueiam os tráfegos UDP e ICMP.

O comando `tracert` tem opções para rastrear o caminho com pacotes UDP (padrão),

ICMP (

`-I`) ou TCP (`-T`). Normalmente o comando `tracert` não está instalado por padrão.

```
[user@host ~]$tracert access.redhat.com...output omitt  
d...  
 4:  71-32-28-145.rcmt.qwest.net                                4  
8.853ms asymm  5  
 5:  dcp-brdr-04.inet.qwest.net                                10  
0.732ms asymm  7  
 6:  206.111.0.153.ptr.us.xo.net                                9  
6.245ms asymm  7  
 7:  207.88.14.162.ptr.us.xo.net                                8  
5.270ms asymm  8  
 8:  ae1d0.cir1.atlanta6-ga.us.xo.net                           6  
4.160ms asymm  7  
 9:  216.156.108.98.ptr.us.xo.net                               10  
8.652ms  
10:  bu-ether13.atlmgamq46w-bcr00.tbone.rr.com                 10  
7.286ms asymm 12  
...output omitted...
```

Cada linha na saída do comando `tracert` representa um roteador ou um salto que o pacote dá da origem até o destino final.

O comando exibe informações para cada salto conforme se tornam disponíveis, incluindo o *tempo de viagem de ida e volta (RTT)* e quaisquer alterações no *tamanho da unidade máxima de transmissão (MTU)*.

A indicação `asymm` significa que o tráfego chegou a esse roteador e retornou do roteador usando rotas diferentes (*assimétricas*). Esses roteadores aqui são

para o tráfego de saída, não para o tráfego de retorno.

Os comandos `tracpath6` e `traceroute -6` são os comandos do IPv6 equivalentes aos comandos `tracpath` e `traceroute`.

```
[user@host ~]$tracpath6 2001:db8:0:2::451
1?: [LOCALHOST] 0.091ms pmtu 1500
1: 2001:db8:0:1::ba 0.214ms
2: 2001:db8:0:1::1 0.512ms
3: 2001:db8:0:2::451 0.559ms reached
Resume: pmtu 1500 hops 3 back 3
```

Solução de problemas de portas e serviços

Os serviços de TCP usam soquetes como pontos de extremidade para comunicação e são compostos de um endereço IP, um protocolo e um número de porta.

Os serviços tipicamente escutam as portas padrão, enquanto os clientes usam uma porta disponível aleatoriamente. Nomes de portas padrão bem conhecidos são listados no arquivo `/etc/services`.

O comando `ss` é usado para exibir as estatísticas de soquete. O comando `ss` substitui a ferramenta `netstat` anterior, parte do pacote `net-tools`, que talvez seja mais conhecida por alguns administradores de sistema, mas nem sempre está instalada.

```
[user@host ~]$ss -ta
State      Recv-Q Send-Q           Local Address:Port           P
eer Address:Port
LISTEN     0      128                *:sunrpc
*:*
LISTEN     0      128                *:ssh
*:*
LISTEN     0      100          127.0.0.1:smtp:
LISTEN     0      128                *:36889
*:*
```



```

ESTAB      0      0      172.25.250.10:ssh      17
2.25.254.254:59392
LISTEN     0      128             :::sunrpc
:::*
LISTEN     0      128             :::ssh
:::*
LISTEN     0      100            ::1:smtp
:::*
LISTEN     0      128             :::34946
:::*

```

- `:::ssh` : a porta usada para SSH está escutando em todos os endereços IPv4. O caractere asterisco (`*`) representa *todos* ao fazer referência a endereços IPv4 ou portas.
- `127.0.0.1:smtp` : a porta usada para SMTP está escutando na interface de loopback `127.0.0.1` IPv4.
- `172.25.250.10:ssh` : a conexão por SSH estabelecida está na interface `172.25.250.10` e se origina em um sistema com o endereço `172.25.254.254`.
- `:::ssh` : a porta usada para SSH está escutando em todos os endereços IPv6. A sintaxe de dois-pontos duplos (`::`) representa todas as interfaces IPv6.
- `::1:smtp` : a porta usada para SMTP está escutando na interface de loopback `::1` IPv6.

Opções para ss e netstat

Opção	Descrição
-n	Mostra números em vez de nomes para interfaces e portas.
-t	Mostra os soquetes de TCP.
-u	Mostra os soquetes de UDP.
-l	Mostra somente os soquetes que estão escutando.
-a	Mostra todos os soquetes (os que estão escutando e os estabelecidos).
-p	Mostra o processo que usa os soquetes.
-A inet	Exibe conexões ativas (mas não soquetes de escuta) para a família de endereços <code>inet</code> .

Ou seja, ignore os soquetes de domínio UNIX locais. Para o comando `ss`, as conexões IPv4 e IPv6 são exibidas.

Para o comando

`netstat`, somente as conexões IPv4 são exibidas.

(O comando

`netstat -A inet6` exibe conexões IPv6, e o comando `netstat -46` exibe IPv4 e IPv6 ao mesmo tempo.)