

Tracking the route

| | |
|---|---|
| <code>ping exampl e.com -c 1</code> | Envia apenas 1 pacote ICMP para testar a conectividade com o destino. |
| <code>ping exampl e.com -c 1 -t 1</code> | Envia 1 pacote ICMP com TTL (Time to Live) definido como 1. |
| <code>tracert exampl e.com</code> | Exibe o caminho completo (hops) até o destino. |
| <code>tracert exampl e.com -w 1</code> | Define o tempo de espera em 1 segundo por resposta de cada hop. |
| <code>tracert exampl e.com -m 1</code> | Limita o número máximo de hops (TTL) a 1. |
| <code>tracert exampl e.com -m 5</code> | Limita o número máximo de hops (TTL) a 5. |
| <code>tracert exampl e.com -m 25 -f 15</code> | Define o TTL inicial como 15 e o TTL máximo como 25. |
| <code>tracert exampl e.com -A</code> | Mostra as informações do sistema autônomo (AS) dos hops. |
| <code>tracert exampl e.com -n</code> | Exibe os endereços IP dos hops sem resolver os nomes DNS. |
| <code>tracert exampl e.com -n -I</code> | Usa pacotes ICMP em vez de UDP para a rota. |
| <code>tracert exampl e.com -n -U</code> | Usa pacotes UDP em vez de ICMP para a rota. |
| <code>tracert exampl e.com -n -T</code> | Usa pacotes TCP em vez de UDP para a rota. |
| <code>tracert exampl e.com -n -T -p 80</code> | Usa pacotes TCP com a porta de destino 80. |
| <code>tracert exampl e.com -n -m 1</code> | Limita o número máximo de hops (TTL) a 1 e exibe o resultado em formato numérico. |
| <code>tracert exampl e.com -n -m 1 -U</code> | Limita o número máximo de hops (TTL) a 1 e usa pacotes UDP. |

firewall

| | |
|--|---|
| <code>iptables -nL</code> | Lista todas as regras de firewall ativas, sem resolver nomes de host ou serviços. |
| <code>iptables -P INPUT DROP</code> | Define a política padrão para INPUT como DROP (bloquear todo o tráfego de entrada). |
| <code>iptables -P INPUT ACCEPT</code> | Define a política padrão para INPUT como ACCEPT (permitir todo o tráfego de entrada). |
| <code>iptables -A INPUT -p tcp --dport 80 -j ACCEPT</code> | Permite conexões TCP na porta 80 (HTTP). |
| <code>iptables -A INPUT -p tcp --dport 80 -j DROP</code> | Bloqueia conexões TCP na porta 80 (HTTP). |
| <code>iptables -A INPUT -p icmp -j ACCEPT</code> | Permite pacotes ICMP (como os usados pelo comando ping). |
| <code>iptables -F</code> | Remove todas as regras de firewall ativas. |
| <code>iptables -A INPUT -p tcp --dport 80 -s 192.168.0.11 -j ACCEPT</code> | Permite conexões TCP na porta 80 (HTTP) somente do IP 192.168.0.11. |



By **lkskaldasklas**

Not published yet.

Last updated 28th January, 2025.

Page 1 of 3.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>

firewall (cont)

| | |
|--|--|
| <pre>iptables -A INPUT -p tcp --dport 80 -s 192.168.0.11 -d 192.168.0.12 -j ACCEPT</pre> | Permite conexões TCP na porta 80 (HTTP) do IP 192.168.0.11 para o IP 192.168.0.12. |
| <pre>iptables -A INPUT -p icmp --icmp -type 8 -j ACCEPT</pre> | Permite pacotes ICMP de tipo 8 (echo request, usados pelo ping). |
| <pre>iptables -A INPUT -p udp -j ACCEPT</pre> | Permite todo o tráfego UDP de entrada. |
| <pre>iptables -A INPUT -p tcp -dport 3306 -s <IP> -j ACCEPT</pre> | Permite conexões TCP na porta 3306 (MySQL) vindas de um IP específico. |
| <pre>iptables -A INPUT -p tcp -dport 3306 -d <IP> -j ACCEPT</pre> | Permite conexões TCP na porta 3306 (MySQL) destinadas a um IP específico. |
| <pre>iptables -A INPUT -p tcp -sport 3306 -j ACCEPT</pre> | Permite conexões TCP com porta de origem 3306 (MySQL). |

ping sweep

| | |
|---|--|
| <pre>for ip in \$(seq 1 254); do ping -c 1 172.16.1.\$ip ;done grep "64 bytes"</pre> | Realiza um ping em todos os IPs do intervalo 172.16.1.1 a 172.16.1.254 e exibe apenas os IPs que responderem com "64 bytes". |
| <pre>for ip in \$(seq 1 254); do ping -c 1 172.16.1.\$ip -w 1;done grep "64 bytes"</pre> | Faz o mesmo que o comando anterior, mas define um tempo limite de 1 segundo para cada ping. |
| <pre>for ip in \$(seq 224 239); do ping -c 1 37.59.174.\$ip -w 1;done grep "64 bytes"</pre> | Realiza um ping nos IPs do intervalo 37.59.174.224 a 37.59.174.239, com um tempo limite de 1 segundo, exibindo somente os IPs que responderem. |
| <pre>fping -a -g 172.16.1.0/24</pre> | Verifica todos os IPs no intervalo 172.16.1.0/24 e exibe apenas os que estão ativos (respondendo ao ping). |



By lkskaldasklas

Not published yet.

Last updated 28th January, 2025.

Page 3 of 3.

Sponsored by [CrosswordCheats.com](https://crosswordcheats.com)

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>

