



8 comandos para redes que todos os utilizadores do Windows devem saber

O Windows inclui muitas ferramentas de linha de comandos para ajudarem os utilizadores a gerirem as configurações das ligações de rede e resolverem problemas. Aqui ficam os 8 comandos relacionados com redes que todos devem saber usar.



Pedro Tróia | [🕒](#) Há 9 meses

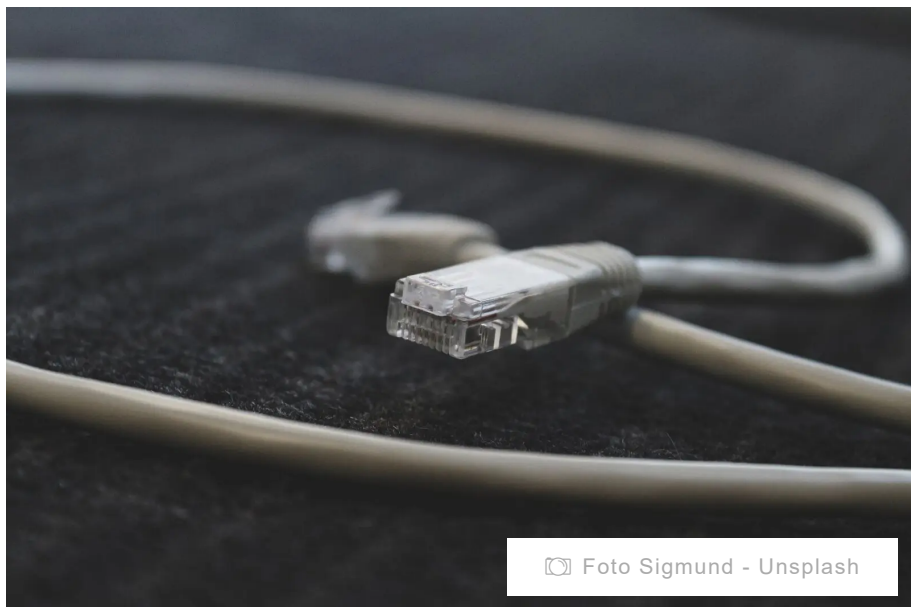


Foto Sigmund - Unsplash

O Windows 10 facilita muito a ligação do computador a uma rede local e à Internet através de ligações com, ou sem, fios. Contudo, por vezes, há alturas em que é necessário gerir as configurações manualmente ou resolver problemas de



Privacidade

conectividade e é nestas alturas em que as ferramentas da linha de comandos dão muito jeito.

Independentemente do problema, o Windows 10 tem, quase de certeza, um comando que o pode ajudar a resolvê-lo. Por exemplo, os comandos 'ipconfig' e 'ping' são as ferramentas mais básicas para ver as definições da ligação de rede e resolver problemas de comunicação. Se estiver com um problema de direccionamento da informação na rede, o comando 'route' pode mostrar a tabela de direccionamento, possibilitando a detecção de problemas e, com o comando 'nslookup' consegue diagnosticar problemas de DNS.

Também estão disponíveis comandos, como o 'arp' que ajuda a resolver problemas com switches e descobrir endereços MAC a partir de endereços IP. O comando 'netstat' permite ver estatísticas para todas as ligações. E pode usar o comando 'netsh' para ver e alterar muitos aspectos das definições das ligações de rede, como ver a configuração actual, redefinir parâmetros, gerir as definições das ligações Ethernet e Wi-Fi, ligar e desligar a firewall e muito mais.

Neste guia para Windows 10 (que também funciona noutras versões), vamos falar de 8 comandos que podem ajudar e gerir e a detectar e resolver problemas de ligação à rede do seu dispositivo.

IPConfig

No Windows 10, o comando 'ipconfig' (Internet Protocol configuration) é uma das ferramentas de rede mais comuns, que lhe permite ver a configuração do protocolo TCP/IP (Transmission Control Protocol/Internet Protocol), utilizado para a



comunicação entre dispositivos e à Internet.

Este comando inclui também opções que permitem fazer várias coisas, como redefinir as definições do DHCP (Dynamic Host Configuration Protocol) e do DNS (Domain Name System).

Ver a configuração da rede

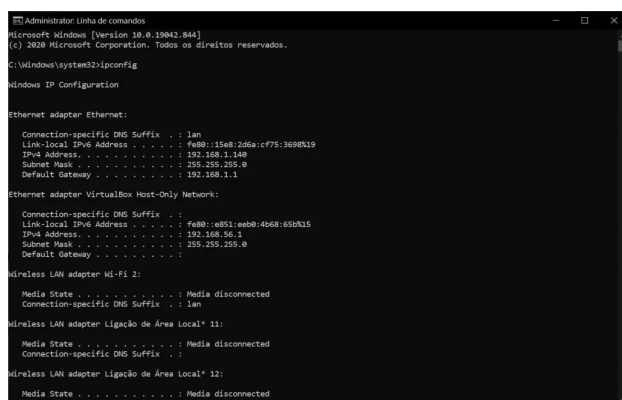
Para começar a usar o comando 'ipconfig', siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter, para ver um resumo da configuração TCP/IP do seu computador:

ipconfig

Dica: Na janela da Linha de Comandos, pode usar o comando 'cls' para a limpar quando já não necessitar da informação que lá estiver.



```
Administrator: Linha de comandos
Microsoft Windows [Version 10.0.19042.844]
(c) 2020 Microsoft Corporation. Todos os direitos reservados.
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . : lan
    Link-local IPv6 Address . . . . . : fe80::15a8:2da:c75:3698%19
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::e6b1:e6b8:4b68:6303%15
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : lan

Wireless LAN adapter Ligação de Área Local* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Wireless LAN adapter Ligação de Área Local* 12:

    Media State . . . . . : Media disconnected
```

Escreva o comando seguinte e prima a tecla Enter, para ver todas as configurações TCP/IP:

ipconfig /all



Depois de completar estes passos, terá uma vista geral de todas as configurações TCP/IP do seu dispositivo.

Redefinir os parâmetros de rede

Para renovar a configuração de rede através da Linha de Comandos, siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter, para remover a configuração de rede que estiver definida:

```
ipconfig /release
```

Escreva o comando seguinte e prima a tecla Enter, para reconfigurar os parâmetros da configuração de rede:

```
ipconfig /renew
```

Depois de completar estes passos, o primeiro comando limpa a configuração de rede e o segundo redefine essa configuração a partir da informação transmitida pelo servidor DHCP (normalmente o router que controla a rede), para resolver problemas de ligação. Se as definições do atribuídas ao seu dispositivo não tiverem expirado, pode dar-se o caso de ser atribuído o mesmo endereço IP ao dispositivo durante a reconfiguração.

Redefinir as configurações do DNS

Para remover e renovar a cache do DNS no Windows, siga estes passos:



Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter, para limpar a cache do sistema DNS no seu dispositivo:

```
ipconfig /flushdns
```

Depois de completar estes passos, todo o conteúdo da cache do sistema DNS que está no Windows será limpo e recarregado. Normalmente, este comando funciona quando não se consegue ligar a outro computador na rede local, ou a um site web, devido à informação que está na cache DNS estar desactualizada.

Ping

O comando 'ping' é outra das ferramentas essenciais para descobrir problemas de ligação em redes locais, ou à Internet, porque permite o envio de pedidos de eco ICMP (Internet Control Message Protocol) para testar a ligação IP a outros dispositivos, quer sejam dispositivos ligados na rede local, ou serviços na Internet.

Testar a ligação de um dispositivo

Para testar a ligação à rede de um dispositivo através do comando 'ping', siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

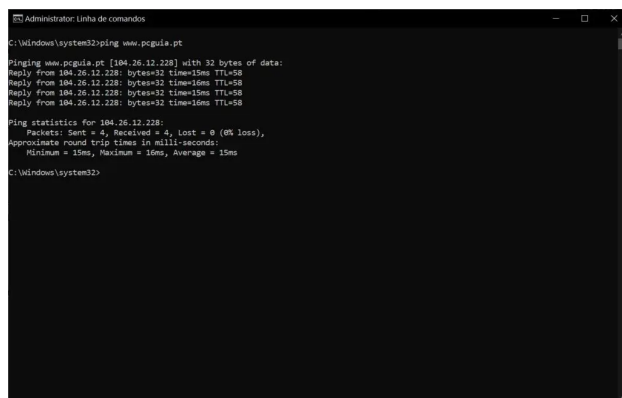
Escreva o comando seguinte e prima Enter, para enviar pedidos de eco para testar a



ligação:

ping IP – ou domínio

No comando, deve substituir 'IP – ou domínio' por um endereço IP ou pelo nome de um domínio que quiser testar.



```
Administrator: Linha de comandos
C:\Windows\system32>ping www.pcguia.pt

Pinging www.pcguia.pt [104.26.12.228] with 32 bytes of data:
Reply from 104.26.12.228: bytes=32 time=15ms TTL=58
Reply from 104.26.12.228: bytes=32 time=15ms TTL=58
Reply from 104.26.12.228: bytes=32 time=15ms TTL=58
Reply from 104.26.12.228: bytes=32 time=15ms TTL=58

Ping statistics for 104.26.12.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 16ms, Average = 15ms

C:\Windows\system32>
```

Por exemplo, este comando testa a comunicação entre um dispositivo e o router que controla a rede:

ping 192.168.1.1

Dica: Pode usar a opção '-a' (por exemplo: ping -a 192.168.1.1) para conseguir ver o nome atribuído a esse dispositivo para além do endereço IP.

Pode também usar o comando seguinte para testar o software de rede do computador:

ping 127.0.0.1

ou

ping loopback

Nota: O endereço IP 127.0.0.1 é o endereço IP definido para o loopback da comunicação num computador. Quando o comando é



Privacidade

executado com este endereço e recebe uma resposta, isso quer dizer que o software de rede do Windows está a funcionar. Se utilizar o endereço IP atribuído ao dispositivo, o resultado será o mesmo.

Depois de completar estes passos, e se receber quatro mensagens de eco a partir do destino quer dizer que o seu dispositivo consegue falar com o dispositivo, cujo endereço IP usou com o comando. Se o comando mostrar uma mensagem de timeout, quer dizer que há problemas na comunicação e o seu dispositivo não consegue comunicar com o dispositivo remoto.

Se estiver com problemas de ligação, comece por fazer ping ao seu computador, para se assegurar de que o software de rede está a funcionar. Depois, teste a ligação ao router, para se assegurar de que não se trata de um problema com a rede local. Por fim, tente fazer ping a um site na Internet, para ficar a saber se há um problema com a ligação à Internet ou com o dispositivo com o qual quer comunicar.

Pode dar-se o caso de o dispositivo remoto estar a bloquear o protocolo ICMP (usado pelo comando 'ping'), assim o resultado do comando será sempre um timeout.

Diagnosticar a perda de pacotes de comunicação

O comando 'ping' inclui uma grande quantidade de opções que podem ser vistas através do comando 'ping /?' e uma delas é a possibilidade de definir o tempo de execução do comando, o que pode ser útil para examinar a perda de pacotes de comunicação quando está a tentar encontrar problemas de ligação.



Para executar o comando 'ping' durante um período de tempo específico, siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter, para o comando 'ping' ser executado até ser interrompido manualmente:

ping IP – ou domínio -t

No comando, deve substituir 'IP – ou domínio' por um endereço IP ou pelo nome de um domínio que quiser testar.

Por exemplo:

Ping 192.168.1.1 -t

Quando quiser parar a execução, utilize a combinação de teclas CTRL+C.

Depois de completar estes passos, conseguirá ver quais os pedidos que foram bem-sucedidos e quais foram os que falharam. Isto pode dar-lhe pistas sobre como continuar a diagnosticar um problema de ligação. Numa rede local, utiliza-se o comando 'ping' para ver quando um serviço deixa de funcionar. Este comando também pode servir para saber rapidamente se um servidor está a funcionar depois de um reinício.

Tracert

Outra das ferramentas do arsenal do Windows 10 é o comando 'tracert' (Trace Route). Este comando serve para ver o



percurso até um dispositivo alvo utilizando uma série de pedidos de eco ICMP. Contudo, e ao contrário do comando 'ping', cada pedido feito pelo 'tracert' inclui um valor TTL (Time To Live), que aumenta em 1 de cada vez, permitindo ver a lista de dispositivos que estão no percurso, quanto tempo demorou cada pedido e a sua duração.

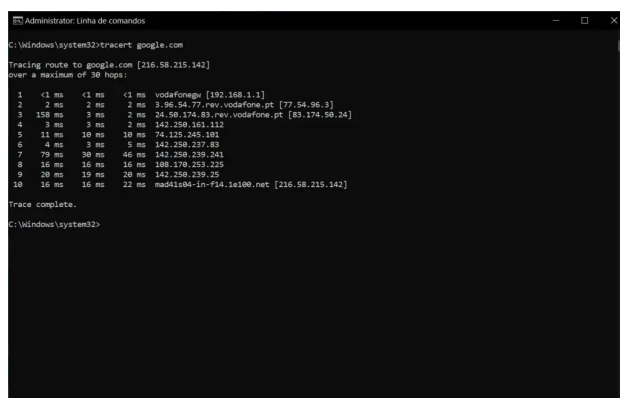
Para ver o percurso até uma máquina de destino, siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter:

tracert IP – ou domínio

No comando, deve substituir 'IP – ou domínio' por um endereço IP ou pelo nome de um domínio que quiser testar.



```
Administrator: Linha de comandos
C:\Windows\system32>tracert google.com

Tracing route to google.com [216.58.215.142]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms    vodafonegw [192.168.1.1]
  1  2 ms     2 ms     2 ms     3.96.54.77.rev.vodafone.pt [77.54.96.3]
  2  158 ms   3 ms     2 ms     24.58.274.82.rev.vodafone.pt [83.174.58.24]
  3  3 ms     3 ms     2 ms     142.259.161.112
  4  11 ms    10 ms    10 ms    74.125.245.181
  5  4 ms     3 ms     5 ms     142.259.237.83
  6  79 ms    30 ms    46 ms    142.259.239.241
  7  16 ms    16 ms    16 ms    142.259.239.225
  8  20 ms    19 ms    20 ms    142.259.239.25
  9  16 ms    16 ms    22 ms    ma041s04-in-F14.1e180.net [216.58.215.142]

Trace complete.
C:\Windows\system32>
```

Por exemplo, neste caso vamos ver o caminho da informação até conseguir comunicar com o site Google.com:

tracert google.com

Pode também ajustar o número de salto até ao destino através do comando seguinte:



Privacidade

`tracert -h número de saltos IP – ou domínio`

No comando, deve substituir 'IP – ou domínio' por um endereço IP ou pelo nome de um domínio que quiser testar. Substitua 'número de saltos' pelo número de saltos que quiser verificar.

Por exemplo, este comando limita a 5 saltos até ao destino:

`tracert -h 5 google.com`

Depois de completar estes passos, conseguirá saber se a máquina de destinos está acessível, ou se há um problema de comunicação pelo caminho.

O comando 'tracert' tem mais opções, que podem ser vistas através do comando 'tracert /?'.

NSLookup

O comando 'nslookup' (Name Server Lookup), pode mostrar-lhe detalhes que o ajudam a encontrar problemas relacionados com DNS. Este comando inclui modos de funcionamento interactivo e não interactivo. O modo mais usado é o não interactivo, o que quer dizer que ira ter de escrever o comando completo para obter a informação de que necessita.

Pode usar este comando para ver o nome e endereço DNS por defeito do dispositivo local, determinar o nome do domínio de um endereço IP e os servidores de nomes de um computador específico.

Para começar a usar o comando 'nslookup', siga estes passos:



Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter para ver o nome DNS e endereço:

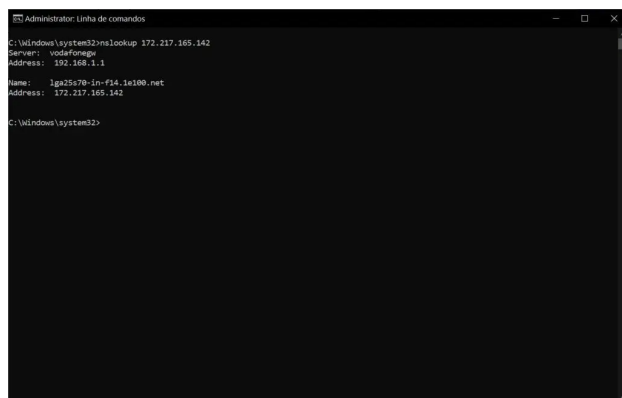
nslookup

Nota: Este comando abre o 'nslookup' em modo interativo.

Confirme a informação do DNS.

Para sair do modo interativo, escreva o seguinte comando e prima Enter:

Exit



```
Administrator: Linha de comandos
C:\Windows\system32>nslookup 172.217.165.142
Server: vodafone.pt
Address: 192.168.1.1

Name:    1g2570-in-f14.1e100.net
Address: 172.217.165.142

C:\Windows\system32>
```

Escreva o comando seguinte e prima a tecla Enter, para determinar o nome e endereço de um servidor específico:

nslookup Endereço IP

Substitua 'Endereço IP' pelo endereço do dispositivo remoto.

Por exemplo, este comando mostra informação de um dispositivo com o endereço 172.217.165.142:



```
nslookup 172.217.165.142
```

Escreva o comando seguinte e prima Enter para determinar o endereço de um servidor específico:

```
nslookup Nome do domínio
```

No comando, substitua 'Nome de domínio' com o endereço do dispositivo remoto.

Por exemplo, neste caso, o comando procura o endereço IP do domínio Google.com:

```
nslookup google.com
```

NetStat

O comando 'netstat' (Network Statistics), mostra estatísticas de todas as ligações de rede. Permite-lhe perceber que portas estão abertas e ligadas de forma a encontrar e monitorizar problemas de rede no Windows 10 e respectivas aplicações.

Através deste comando, pode ver que ligações estão activas e que portas estão em modo de escuta. Pode ver também estatísticas de um adaptador de rede e dos protocolos. Pode ver também a tabela de redireccionamento actual e muito mais.

Para começar a usar o comando 'netstat', siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter, para ver todas as ligações TCP que estão activas:



netstat

Pode também escrever o comando seguinte para mostrar as ligações activas, mostrando os endereços IP e número da porta, em vez de estar a tentar descobri-los:

netstat -n

Pode ainda usar esta comando para recarregar a informação automaticamente ao fim de algum tempo:

netstat -n tempo

No comando, substitua a palavra 'tempo' por um número (segundos) findo o qual a informação é mostrada outra vez.

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1826	127.0.0.1:55525	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55527	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55528	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55529	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55530	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55532	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55533	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55534	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55535	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55536	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55537	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55538	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55539	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55540	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55541	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55542	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55543	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55544	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55545	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55546	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55547	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55548	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55549	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55550	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55551	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55552	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55553	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55554	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55555	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55556	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55557	TIME_WAIT
TCP	127.0.0.1:1826	127.0.0.1:55559	TIME_WAIT

Neste exemplo, é mostrada nova informação a cada 5 segundos:

netstat -n 5

Nota: Quando quiser interromper a execução do comando, utilize a combinação de teclas CTRL+C.

Depois de executar o comando, será mostrada uma lista de todas as ligações activas organizadas em quatro colunas:



Proto: Mostra o protocolo utilizado na ligação, TCP ou UDP.

Local Address: Mostra o endereço IP do dispositivo, seguido de dois pontos com o número do port (porta) dessa ligação. Se tiver duas vezes dois pontos indica um endereço IPV6. Se aparecer 0.0.0.0 também se refere ao endereço local.

Foreign Address: Mostra o endereço IP do computador remoto, acompanhado pelo tipo de ligação utilizada (por exemplo: https, http, microsoft-ds, wsd).

State: Indica se a ligação está activa (established), se o port foi fechado (time_wait) e se o programa não fechou o port (close_wait). Outros estados incluem: 'closed', 'fin_wait_1', 'fin_wait_2', 'last_ack', 'listen', 'syn_received', 'syn_send' e 'timed_wait'.

ARP

O Windows mantém uma tabela arp (Address Resolution Protocol), onde são guardadas informações acerca das ligações entre endereços IP e MAC (Media Access Control) que o sistema tenha conseguido resolver. O comando 'arp' permite toda a tabela, modificá-la e utilizá-la para ver o endereço MAC de um computador remoto.

Normalmente, não é necessário preocupar-se com os endereços MAC, mas pode haver alturas em que esta informação pode ser útil. Por exemplo, quando está a tentar resolver problemas na rede, ou quer filtrar conteúdos específicos em certos dispositivos na rede.

Para começar a usar o comando 'arp', siga estes passos:



Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o comando seguinte e prima a tecla Enter, para ver a tabela arp:

arp -a

Para determinar o endereço IP, use este comando:

arp -a IP

Substitua 'IP' por um endereço IP.

```

Administrator: Linha de comandos
C:\Windows\system32\arp -a

Interface: 192.168.56.1 --- eth0
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-0b    static
224.0.0.252           01-00-5e-00-00-0c    static
224.0.0.3             01-00-5e-00-00-03    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.1.148 --- Wi-Fi
Internet Address      Physical Address      Type
192.168.1.1           2c-9d-16-d2-20-ec    dynamic
192.168.1.114         08-11-32-00-03-64    dynamic
192.168.1.115         a3-86-a3-91-5c-ca    dynamic
192.168.1.164         a4-77-33-93-e7-9a    dynamic
192.168.1.209         38-5d-52-07-90-7f    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-0b    static
224.0.0.252           01-00-5e-00-00-0c    static
224.0.0.3             01-00-5e-00-00-03    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Windows\system32>
  
```



PARTILHAR



Por exemplo, este comando revela o endereço MAC de 192.168.1.114:

arp -a 10.1.4.108

Se quiser usar outras opções com o comando 'arp', escreva 'arp /?' e prima a tecla enter.

Depois de completar estes passos, conseguirá ver toda a tabela arp e o endereço MAC de um dispositivo com um endereço IP específico.

Route

Verifique a velocidade da Internet

Privacidade

O comando 'route' mostra a tabela routing (direccionamento) que permite ao Windows perceber a rede e comunicar com outros dispositivos e serviços. Este comando também oferece algumas opções para modificar e limpar a tabela, se for necessário.

Tal como com o comando 'arp', tipicamente os utilizadores não têm de se preocupar com a tabela de routing, mas este comando pode ajudar a encontrar e resolver problemas na rede.

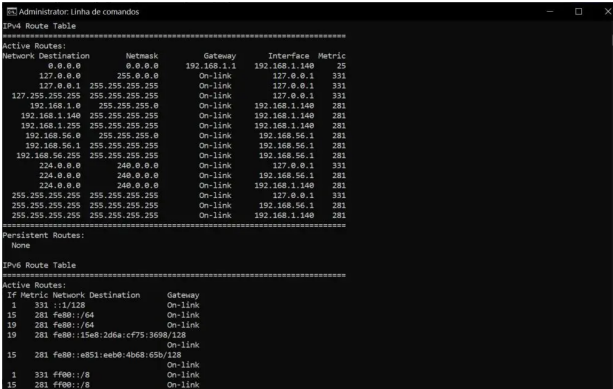
Para ver ou apagar o conteúdo da tabela de routing, siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Escreva o seguinte comando e prima a tecla enter:

route print

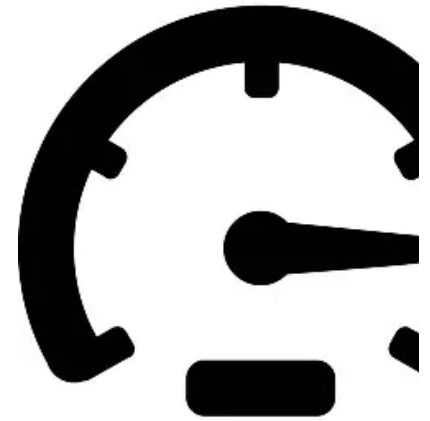
Confirme a informação que está na tabela.



```
Administrator: Linha de comandos
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.148    25
127.0.0.0                  255.0.0.0        On-link         127.0.0.1        331
127.0.0.1                  255.255.255.255 On-link         127.0.0.1        331
127.255.255.255            255.255.255.255 On-link         127.0.0.1        331
192.168.1.0                255.255.255.0    On-link         192.168.1.148    281
192.168.1.148              255.255.255.255 On-link         192.168.1.148    281
192.168.1.255              255.255.255.255 On-link         192.168.1.148    281
192.168.56.0               255.255.255.0    On-link         192.168.56.1     281
192.168.56.1               255.255.255.255 On-link         192.168.56.1     281
192.168.56.255             255.255.255.255 On-link         192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link         127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link         192.168.56.1     281
224.0.0.0                  240.0.0.0        On-link         192.168.1.148    281
255.255.255.255            255.255.255.255 On-link         127.0.0.1        331
255.255.255.255            255.255.255.255 On-link         192.168.56.1     281
255.255.255.255            255.255.255.255 On-link         192.168.1.148    281
Persistent Routes:
None
IPv6 Route Table
=====
Active Routes:
IP Metric Network Destination      Gateway
1 331 ::1 ::1/128             On-link
15 281 fe80::/64             On-link
19 281 fe80::/64             On-link
19 281 fe80::5a8:2d6a:c75:3698/128 On-link
15 281 fe80::a851:aabb:4b68:650/128 On-link
1 331 ff00::/8              On-link
15 281 ff00::/8              On-link
```

Opcionalmente, pode limpar o conteúdo da tabela através deste comando:

route -f



Apoio

webhr



Privacidade

Nota: Quando executa este comando, o dispositivo perde a ligação à rede, porque o dispositivo deixa de perceber a topologia da rede. Depois de executar o comando, reinicie o computador para permitir ao software de rede reconstruir a tabela de routing. Normalmente, não há necessidade de limpar esta tabela, a menos que tenha modificado algumas das entradas e necessita de repor a tabela.

Pode também usar o comando 'route /?' para ver uma lista de opções disponíveis, incluindo as opções que permitem a alteração da métrica da rede, especificar uma gateway, adicionar uma nova rota e muito mais. No entanto, só é aconselhável fazer alterações se perceber como é que funciona uma rede.

Netsh

O comando 'netsh' (Network Shell) é um comando que permite alterar praticamente todas as definições de rede no computador. Por exemplo, pode usá-lo para ver a configuração actual da rede, gerir ligações sem fios, repor as definições do software de rede para resolver a maioria dos problemas que podem surgir, ligar ou desligar a firewall e muito mais.

Para começar a usar o comando 'netsh', siga estes passos:

Aceda ao menu 'Iniciar', escreva 'Linha de comandos' e clique com botão direito do rato no primeiro resultado que aparecer e escolha a opção 'Executar como administrador'.

Insira o comando seguinte e prima a tecla enter para ver uma lista de opções (contextos) e sintaxe do comando 'netsh':

```
netsh /?
```



Para ver a lista de subcomandos (subcontexts) de uma opção específica escreva:

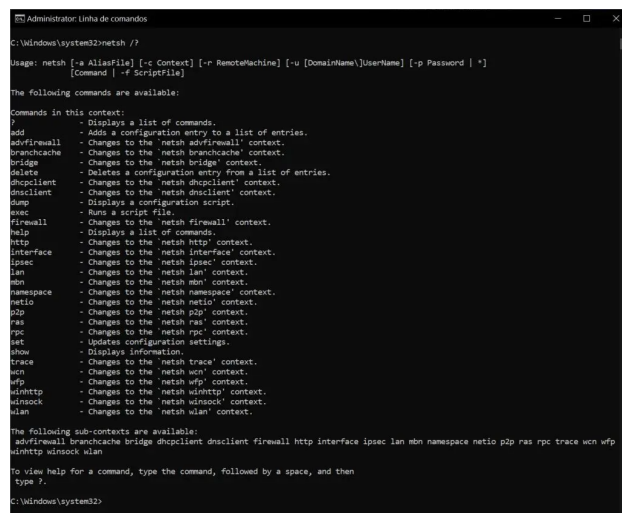
netsh contexto-comando

Substitua as palavras 'contexto-comando' pelo comando para ver mais opções.

Por exemplo, este comando mostra as opções disponíveis para gerir a firewall do Windows usando o 'netsh':

netsh advfirewall /?

Após seguir estes passos, vai conseguir navegar os contextos e subcontextos do comando 'netsh' para conseguir gerir as definições de rede.



```
C:\Windows\system32>netsh /?

Usage: netsh [-s AliasFile] [-c Context] [-r RemoteMachine] [-u [DomainName\]UserName] [-p Password | *]
[Command] [-f ScriptFile]

The following commands are available:

Commands in this context:
?           - Displays a list of commands.
add         - Adds a configuration entry to a list of entries.
advfirewall - Changes to the 'netsh advfirewall' context.
branchcache - Changes to the 'netsh branchcache' context.
bridge      - Changes to the 'netsh bridge' context.
delete      - Deletes a configuration entry from a list of entries.
dhcpcclient - Changes to the 'netsh dhcpcclient' context.
disclient   - Changes to the 'netsh disclient' context.
dump        - Displays a configuration script.
exec        - Runs a script file.
firewall    - Changes to the 'netsh firewall' context.
help        - Displays a list of commands.
http        - Changes to the 'netsh http' context.
interface   - Changes to the 'netsh interface' context.
ipsec       - Changes to the 'netsh ipsec' context.
lan         - Changes to the 'netsh lan' context.
mnm         - Changes to the 'netsh mnm' context.
namespace   - Changes to the 'netsh namespace' context.
netio       - Changes to the 'netsh netio' context.
p2p         - Changes to the 'netsh p2p' context.
ras         - Changes to the 'netsh ras' context.
rpc         - Changes to the 'netsh rpc' context.
set         - Updates configuration settings.
show        - Displays information.
trace       - Changes to the 'netsh trace' context.
wcn         - Changes to the 'netsh wcn' context.
wfp         - Changes to the 'netsh wfp' context.
winhttp     - Changes to the 'netsh winhttp' context.
winsock     - Changes to the 'netsh winsock' context.
wlan        - Changes to the 'netsh wlan' context.

The following sub-contexts are available:
advfirewall branchcache bridge dhcpcclient disclient firewall http interface ipsec lan mnm namespace netio p2p ras rpc trace wcn wfp
winhttp winsock wlan

To view help for a command, type the command, followed by a space, and then
type /?.

C:\Windows\system32>
```

Repor o software de rede do Windows

Para repor as definições do software de rede, e assim resolver vários problemas, faça o seguinte:

Na linha de comandos, insira o comando seguinte e prima a tecla Enter:

netsh winsock reset



Privacidade

Reinicie o computador.

Depois de completar estes passos, a configuração do software que suporta a comunicação de rede no Windows será reposta para os valores de fábrica.

Exportar e importar a configuração de rede

Para exportar a configuração de rede através do comando 'netsh', siga estes passos:

Na Linha de Comandos, insira o comando seguinte e prima tecla Enter para exportar a configuração actual da rede para um ficheiro:

```
netsh -c interface dump>Caminho\ficheiro.txt
```

No comando, substitua 'caminho\ficheiro.txt' pelo caminho e pelo nome do ficheiro onde quer guardar a informação da configuração de rede.

Por exemplo, este comando guarda a informação num ficheiro chamado info_rede.txt:

```
netsh -c interface dump>c:\info_rede.txt
```

Depois de completar estes passos, pode abrir o ficheiro criado num qualquer editor de texto para ver a informação lá contida.

Importar a configuração de rede

Para importar a configuração de rede a partir de um ficheiro através do comando 'netsh', siga estes passos:

Na Linha de Comandos, insira o comando seguinte para importar a configuração de rede:



```
netsh -f Caminho\ ficheiro.txt
```

No comando, substitua 'caminho\ ficheiro.txt' pelo caminho e pelo nome do ficheiro onde está informação da configuração de rede.

Por exemplo, este comando lê a informação num ficheiro chamado info_rede.txt:

```
netsh -f c:\info_rede.txt
```

Depois de completar estes passos, a nova configuração de rede será importada para o Windows.

Ligar e desligar a firewall do Windows

Para ligar a firewall no Windows através do comando 'netsh', siga estes passos:

Escreva o comando seguinte na Linha de Comandos e prima a tecla Enter:

```
netsh advfirewall set currentprofile state on
```

Depois de completar este passo, a firewall do Windows será ligada no computador.

Desligar a firewall

Para desligar a firewall no Windows através do comando 'netsh', siga estes passos:

Escreva o comando seguinte na Linha de Comandos e prima a tecla Enter:

```
netsh advfirewall set currentprofile state off
```

Depois de executar este comando, a firewall do Windows será desligada.



Existem muitos mais comandos que o podem ajudar a resolver problemas de ligação de rede no Windows. Este guia serve para dar uma ideia inicial do que se consegue fazer usando apenas a Linha de Comandos usando apenas os comandos mais básicos.

ETIQUETAS # LINHA DE COMANDO # REDE

< ARTIGO ANTERIOR

ARTIGO SEGUINTE >



**Limitação de Hash Rate da
Nvidia GeForce RTX 3060
12GB ultrapassada**

**Fidelidade e Instituto
Superior Técnico lançam
programa de requalificação
remunerado com
certificação OutSystems**



Deixe um comentário

O seu endereço de email não será publicado. Campos obrigatórios marcados com *

Publique o seu comentário

Nome

Email

Website

Publicar comentário

Também lhe pode interessar



Privacidade