

TraceTCP v1.0.3

☐☐ Manual TraceTCP v1.0.3 — Windows CMD

☐☐ 1. Downloads necessários

Arquivo	Link	Obs
tracetcp v1.0.3	https://github.com/0xcafed00d/tracetcp/releases	Base/t/tracetcp.exe
WinPcap 4.1.3	https://www.winpcap.org/install/default.htm	DLL obrigatória

“ ⚠ **O WinPcap é OBRIGATÓRIO.** O tracetcp não funciona sem ele — ele substitui o uso de raw sockets que a Microsoft removeu a partir do XP SP2.

☐☐ 2. Instalação passo a passo

Passo 1 — Instalar o WinPcap

1. Baixe o instalador do WinPcap no link acima
2. Execute `WinPcap_4_1_3.exe` como **Administrador**
3. Siga o assistente de instalação (Next → Next → Finish)
4. Reinicie o computador se solicitado

Passo 2 — Instalar o tracetcp.exe

1. Baixe o arquivo `tracetcp.exe` na página de releases do GitHub
2. Copie o executável para uma pasta no PATH do sistema, por exemplo:

```
C:\Windows\System32\
```

Ou crie uma pasta dedicada e adicione ao PATH manualmente:

```
C:\Tools\tracetc\
```

3. Executando via CMD

“ ⚠ **Sempre abra o CMD como Administrador** — o tracetc exige privilégios elevados para capturar pacotes.

Sintaxe geral

```
tracetc.exe host[:porta]:serviço [opções]
```

- Se nenhuma porta for informada, assume **porta 80 (HTTP)** por padrão.

4. Opções disponíveis

Opção	Descrição
-?	Exibe a ajuda
-c	Modo condensado (saída resumida)
-h N	Inicia o trace a partir do hop N
-m N	Máximo de hops até o destino
-n	Desativa resolução reversa de DNS em cada nó
-p N	Número de pings por hop (padrão: 3)
-r p1 p2	Múltiplos traces de porta p1 até p2
-t N	Timeout em milissegundos para cada resposta
-v	Exibe a versão
-F	Desativa o timer anti-flood (traces mais rápidos)

Opção	Descrição
<code>-s p1 p2</code>	Modo scan de porta fácil (equivale a <code>-cnr p1 p2 -h 128 -m 1 -p 1</code>)
<code>-g endereço</code>	Usa um host específico como gateway

☐ 5. Exemplos práticos — Trace com porta para DNS

O DNS usa a **porta 53**. Abaixo exemplos reais para testar conectividade TCP na porta 53 até servidores DNS.

▶ Teste para o DNS público do Google (8.8.8.8) na porta 53

```
tracetcp.exe 8.8.8.8:53
```

▶ Teste para o DNS público da Cloudflare (1.1.1.1) na porta 53

```
tracetcp.exe 1.1.1.1:53
```

▶ Teste para o seu DC/DNS interno (exemplo minidc.int)

```
tracetcp.exe 192.168.1.1:53
```

▶ Sem resolução reversa de DNS (mais rápido)

```
tracetcp.exe 8.8.8.8:53 -n
```

☐ 6. Interpretando a saída

```
Tracing route to 8.8.8.8 on port 53  
Over a maximum of 30 hops.
```

```

1    1 ms    1 ms    1 ms    192.168.1.1          <- Gateway local2    9 ms    10 ms    8 ms
10.0.0.1          <- Roteador do ISP3    11 ms    12 ms    11 ms    189.x.x.x          <- Nó
intermediário
...
N    Destination Reached in 25 ms.          <- Destino alcançado    Connection established
to 8.8.8.8        <- Conexão TCP estabelecida
Trace Complete.

```

Resultado	Significado
Destination Reached	Porta aberta e conexão TCP estabelecida ☐
Destination Reached + port is closed	Host alcançado mas porta fechada ou filtrada ⚠
* * * Request timed out	Hop bloqueando ICMP ou firewall dropando o pacote ☐

⚠ 7. Observações importantes

- **Execute sempre como Administrador** — sem isso o WinPcap não consegue capturar pacotes
- O tracetcp **não funciona via dial-up** (limitação do WinPcap)
- Testado no Windows XP, Vista, 7, 10 e 11
- DNS na porta 53 TCP é para transferência de zona e consultas grandes — alguns firewalls bloqueiam TCP/53 mas liberam UDP/53 (o tracetcp usa TCP)
- Se o destino for alcançado mas a porta aparecer como fechada, pode ser que o host não aceite conexões com TTL=0; o tracetcp v1.0.3 reenvia automaticamente com TTL alto para confirmar

Revisão #1

Criado em Tue, Mar 24, 2026 4:48 PM por Jean Vieira

Atualizado em Tue, Mar 24, 2026 4:54 PM por Jean Vieira