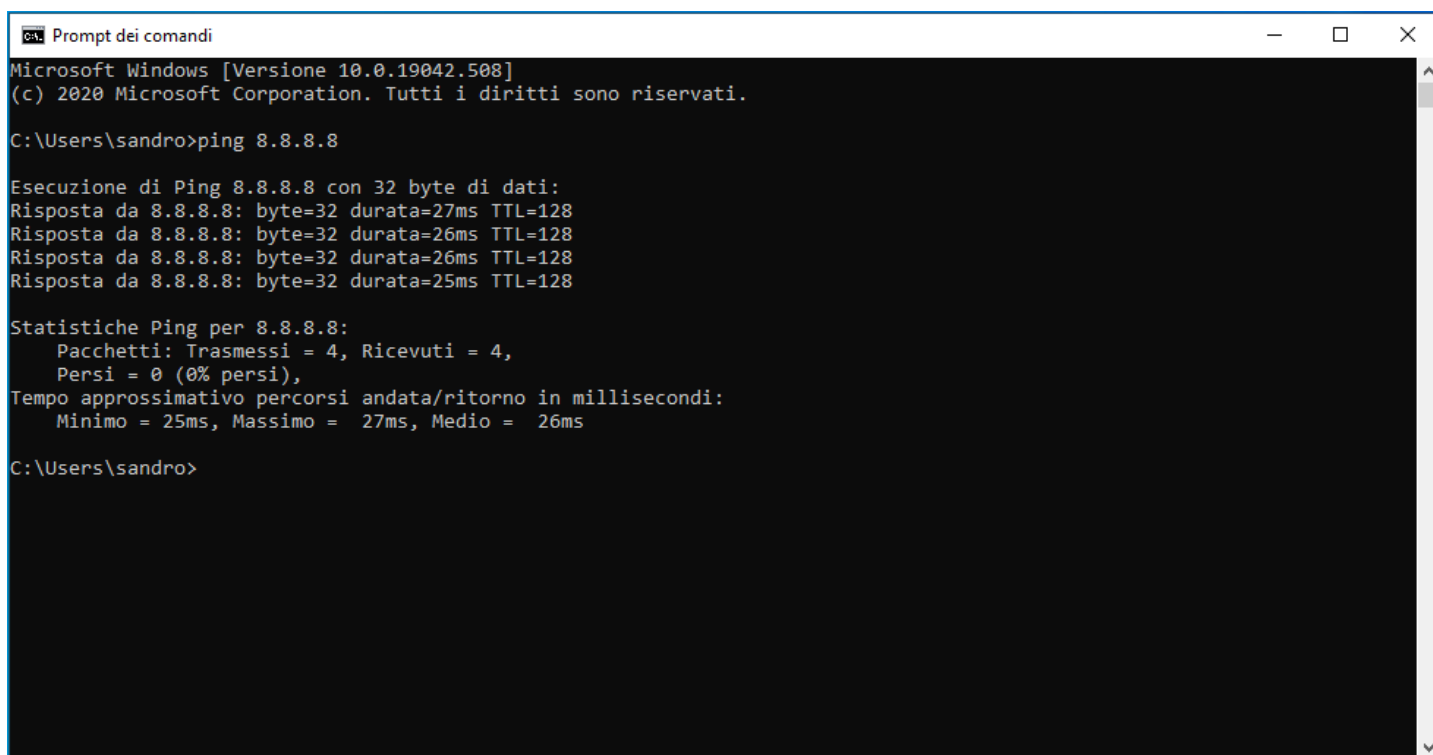


I principali comandi DOS di rete che ogni amministratore Windows dovrebbe conoscere

Windows · Sandro C.



```
Microsoft Windows [Versione 10.0.19042.508]
(c) 2020 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\sandro>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=27ms TTL=128
Risposta da 8.8.8.8: byte=32 durata=26ms TTL=128
Risposta da 8.8.8.8: byte=32 durata=26ms TTL=128
Risposta da 8.8.8.8: byte=32 durata=25ms TTL=128

Statistiche Ping per 8.8.8.8:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 25ms, Massimo = 27ms, Medio = 26ms

C:\Users\sandro>
```

Usando il Prompt dei Comandi di Windows è possibile accedere a numerose utilità tramite righe di comando. Ecco quali sono quelle più importanti che ogni amministratore di rete dovrebbe conoscere.

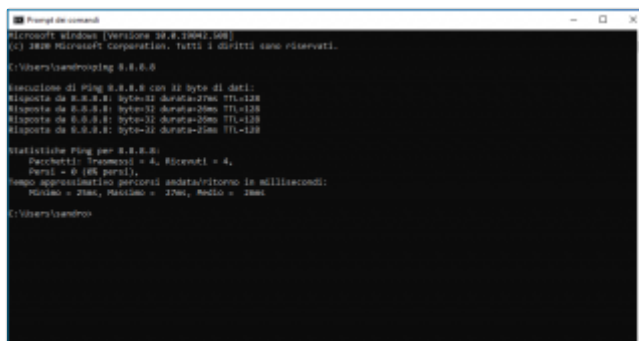
Di seguito riportiamo una panoramica dei principali **comandi di rete** da effettuare sul **Prompt dei Comandi**. Una serie di strumenti utili per la **verifica delle reti TCP/IP** in ambiente Windows.

Ogni **comando di rete** riportato nella presente guida deve essere eseguito dal **Prompt dei Comandi**, raggiungibile facilmente digitando "**cmd**" nel campo di ricerca di Windows e, successivamente, digitando il comando in questione nella finestra del DOS e premendo invio sulla tastiera.

Ecco quindi tutti i **comandi di rete DOS** che ogni amministratore di Windows dovrebbe conoscere.



Ping



```
Microsoft Windows [versione 10.0.19042.508]
(c) 2020 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ping 8.8.8.8

Esecuzione di Ping 8.8.8.8 con 32 byte di dati:
Risposta da 8.8.8.8: byte=32 durata=27ms TTL=128
Risposta da 8.8.8.8: byte=32 durata=26ms TTL=128
Risposta da 8.8.8.8: byte=32 durata=26ms TTL=128
Risposta da 8.8.8.8: byte=32 durata=26ms TTL=128

Statistiche Ping per 8.8.8.8:
Pacchetti: Transmessi = 4, Ricevuti = 4,
Perdi = 0 (0% persi),
Tempo approssimativo percorso andata/ritorno in millisecondi:
Minimo = 26ms, Massimo = 27ms, Medio = 26ms

C:\Users\user>
```

Il comando **ping** è probabilmente quello più conosciuto ma non per questo meno importante. Viene usato per testare la capacità di comunicazione tra un host di rete e un altro.

Per lanciare questo comando è sufficiente inserire il comando "**ping**", seguito dal nome o dall'indirizzo IP dell'host di destinazione. Qualora non si conosca l'IP, in alcuni casi è possibile usare il nome a dominio, ad esempio per **pingare un sito web**.

Es. "ping 8.8.8.8" oppure "ping google.com" per pingare google.com.

Qualora non siano presenti problemi di rete o firewall che ne impediscano il completamento, l'host remoto risponderà al ping con quattro pacchetti da 32 bytes per confermare l'esistenza di un percorso di rete valido e funzionante tra i due host.

Ognuno di questi pacchetti conterrà le seguenti informazioni:

Bytes: dimensioni del pacchetto;

Durata: tempo in millisecondi che intercorre tra la richiesta e la risposta;

TTL (Time To Live) numero di passaggi che il pacchetto ha eseguito per arrivare a destinazione.

In caso di problemi invece si riceverà il messaggio "**Richiesta scaduta**".

NetStat



```
Microsoft Windows [Versione 10.0.10240.960]
(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\vaadm\cmd.exe
C:\Users\vaadm>netstat /?

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

netstat [-a] [-b] [-e] [-f] [-s] [-p] [-r] [-t] [-x] [-y] [-v] [-w] [intervalo]

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'assegnabile coinvolto nella creazione di ogni connessione e
  porta di ascolto. In alcuni casi, nomi di assegnabili non
  può componenti indipendenti e in questi casi il
  sequenza di componenti coinvolti nella creazione della connessione
  o la porta di ascolto. In questo caso, l'assegnabile
  il nome è in {} nella parte inferiore. In alto è il componente che ha chiamato,
  e così via fino al raggiungimento di TCP/IP. Se questa opzione
  può richiedere molto tempo e avere esito negativo, è meno che non siano sufficienti
  autorizzazioni.
-e Visualizza le statistiche Internet. È possibile cambiare
  opzione.
-f Visualizza nomi di dominio completi (qname) per stranieri
  indirizzi.
-s Visualizza indirizzi e numeri di porta in formato numerico.
-t Visualizza l'ID del processo proprietario associato a ogni connessione.
-p mostra le connessioni per il protocollo specificato da proto; proto
  può essere qualsiasi: TCP, UDP, ICMP, o IPSEC. Ha esito con
  opzione per la visualizzazione delle statistiche per protocollo. Proto può essere qualsiasi:
  IP, ICMP, ICMPv6, TCP, UDPv6, OSPF o OSPFv6.
-r Visualizza tutte le connessioni, le porte di ascolto e i binding
```

Le statistiche possono essere utili ad individuare la causa di eventuali **problemi nelle connessioni di rete**. A tal fine è possibile usare comando "**netstat**" per verificare tutte le informazioni relative alle connessioni in entrata e uscita: indirizzo IP locale e porta usata, indirizzo di collegamento e stato della connessione che può essere established (stabilita), time_wait (in attesa) o listening (in ascolto).

Se ciò non bastasse, è possibile usare il comando **netstat** con alcune opzioni per ottenere informazioni più dettagliate, ecco alcuni esempi:

- a**: si otterrà un elenco delle connessioni aperte e le relative porte;
- e**: saranno elencati alcune informazioni sui pacchetti ricevuti e trasmessi;
- n**: verranno riportati gli indirizzi IP locali ed esterni con le rispettive porte usate;
- r**: per conoscere le tabelle di routing;
- s**: riporterà una serie informazioni riassuntive relative ai protocolli di rete usati, tra cui: TCP, UDP, IP, ICMP.

Per ottenere una lista completa delle opzioni utilizzabili in combinazione con il comando netstat è possibile digitare:

netstat /?

ARP

```
Microsoft Windows [Versione 10.0.10240.960]
(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\vaadm>arp

Consente di visualizzare e modificare le tabelle di conversione da indirizzi IP
a indirizzi fisici utilizzate dal protocollo ARP (Address Resolution Protocol).

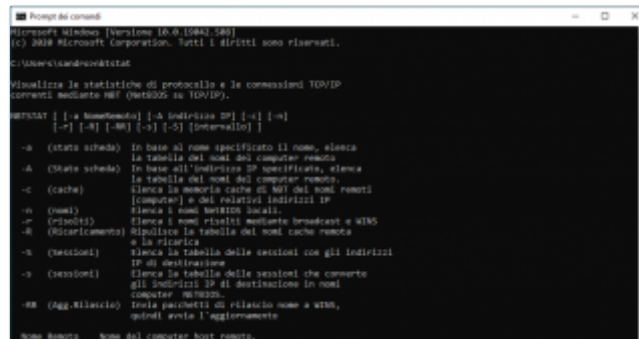
arp [-a] [-n] [-s] [-d] [-i] [-m] [-o] [-x] [-v] [-w] [-c] [-f] [-g] [-h] [-l] [-m] [-n] [-p] [-r] [-s] [-t] [-v] [-w] [-x] [-y] [-z] [-?]

-a Visualizza le voci ARP correnti ottenibile dai dati del
  protocollo. Se è specificato ind_int, verranno visualizzati
  solo gli indirizzi IP e fisico del computer specificato, se
  sono presenti alla interfaccia di rete che utilizza ARP,
  verranno visualizzate le voci di ogni tabella ARP.
  analogo a -a.
-b Visualizza le voci ARP correnti in modalità dettagliata.
  vengono visualizzate anche tutte le voci non valide e le
  voci relative all'interfaccia localhost.
-ind_int Specifica un indirizzo Internet.
-i ind_if Visualizza le voci ARP per l'interfaccia di rete specificata
  da ind_if.
-d Elimina l'host specificato da ind_int. Da ind_int è
  possibile utilizzare il carattere jolly asterisco (*) per
  eliminare tutti gli host.
-f Aggiunge l'host e associa l'indirizzo Internet ind_int
  all'indirizzo fisico ind_if. L'indirizzo fisico è un numero
  esadecimale di 6 byte separati da trattini.
```

Tramite il **protocollo di risoluzione degli indirizzi (ARP)** è possibile **mappare gli indirizzi IP agli indirizzi MAC**. Poiché i dispositivi Windows conservano una cache ARP che contiene i risultati delle ultime query, è possibile visualizzarne il

contenuto usando il comando "**arp -a**". Inoltre, qualora avessi problemi di comunicazione con un host specifico, è possibile anche aggiungere l'indirizzo IP dell'host remoto al comando **arp -a**.

NbtStat



```
Microsoft Windows [Versione 6.0.6002.580]
(c) 2009 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\valter>nbtstat

Visualizza le statistiche di protocollo e le connessioni TCP/IP
correnti mediante NBT (NetBIOS su TCP/IP).

NBTSTAT [-a nomehost] [-A indirizzo IP] [-s] [-e]
[-r] [-R] [-M] [-c] [-S] [Intervallo]

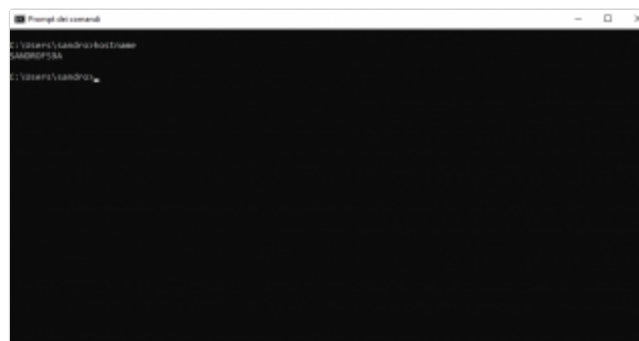
-a (stato scheda) In base al nome specificato il nome, ricerca
la tabella dei nomi del computer remoto.
-A (stato scheda) In base all'indirizzo IP specificato, ricerca
la tabella dei nomi del computer remoto.
-c (cache) Ricerca la memoria cache di NBT dei nomi remoti
[computer] e dei relativi indirizzi IP.
-e (nomi) Ricerca i nomi NetBIOS locali.
-r (risolti) Ricerca i nomi risolti mediante broadcast e WINS.
-R (ricaricamento) Ricarica la tabella dei nomi cache remoto
e la ricarica.
-S (sessioni) Ricerca la tabella delle sessioni con gli indirizzi
IP di destinazione.
-s (sessioni) Ricerca la tabella delle sessioni che converte
gli indirizzi IP di destinazione in nomi
computer.
-RR (Agg. rilascio) Invia pacchetti di rilascio nome a NBT,
quindi evita l'aggiornamento.

Nome remoto Nome del computer host remoto.
```

Sarai certamente a conoscenza del fatto che ad ogni computer equipaggiato con un sistema operativo Windows viene attribuito un nome computer, talvolta denominato come NetBIOS.

Poiché il protocollo NetBIOS su TCP/IP potrebbe interrompersi occasionalmente, il comando "**nbtstat**" può essere un valido aiuto per diagnosticare il problema. A tal proposito il comando "**nbtstat -n**", ad esempio, mostrerà tutti i nomi NetBIOS utilizzati da un dispositivo, mentre "**nbtstat -r**" mostrerà quanti nomi NetBIOS il dispositivo è stato in grado di risolvere recentemente.

Hostname



```
Microsoft Windows [Versione 6.0.6002.580]
(c) 2009 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\valter>hostname
valter-PC
```

Se invece stai cercando di **reperire solo il nome di assegnato a un PC Windows**, il modo più veloce per farlo è usare il comando "**hostname**" e premere invio.

Tracert



```
Windows [comando]
C:\Users\andros>tracert
 Sintassi: tracert [-d] [-h max_hops] [-j elenca_hops] [-w timeout]
              [-k] [-S indirig] [-I] [-6] nome_destinazione
 Opzioni:
 -d          Non risolve gli indirizzi in nome host.
 -h max_hops Numero massimo di punti di passaggio per ricercare
              la destinazione.
 -j elenca_hops Instradamento libero lungo l'elenco hops (solo IPv4).
 -w timeout Timeout in millisecondi per ogni risposta.
 -k          Traccia percorso andata e ritorno (solo IPv4).
 -S indirig  Indirizzo di origine da utilizzare (solo IPv6).
 -I         Dopo l'uso di IPv6.
 -6         Dopo l'uso di IPv4.
C:\Users\andros>
```

Tracert o "**Trace Route**", è un comando utile ad **esaminare il percorso di un host remoto**. Per grandi linee, permette di conoscere i router attraverso i quali passano i pacchetti di dati. Se, ad esempio, uno di questi non dovesse rispondere, usando questo comando si potrà individuare dove risiede il problema di comunicazione.

IpConfig

```
Windows [comando]
C:\Users\andros>ipconfig
 Configurazione IP di Windows

 Scheda Ethernet Ethernet:
 Suffisso DNS specifico per connessione: localdomain
 Indirizzo IPv4 . . . . . : 192.168.1.100
 Indirizzo IPv6 temporaneo . . . . . : fe80::220:444:0:7181::2475:6408
 Indirizzo IPv6 locale rispetto al collegamento . . . . . : fe80::220:444:0:7181::2475:6408
 Indirizzo IPv6 . . . . . : fe80::220:444:0:7181::2475:6408
 Indirizzo DHCP . . . . . : 192.168.1.100
 Subnet mask . . . . . : 255.255.255.0
 Gateway predefinita . . . . . : fe80::220:444:0:7181::2475:6408
 192.168.1.1
C:\Users\andros>
```

Uno dei comandi più usati è certamente "**ipconfig**". Questo, nella sua espressione più semplice, mostrerà tutte le **informazioni di configurazione IP** di qualsiasi dispositivo di rete nel nostro sistema, come ad esempio la scheda ethernet, il gateway o il router. Risulta particolarmente utile quando si usano connessioni di tipo DHCP per conoscere l'indirizzo IP assegnato.

Se usato insieme all'opzione **/all** si otterranno informazioni più dettagliate, tra cui indirizzo MAC, DNS e indirizzo IPv6.

Ma il comando "**ipconfig**" può aiutarti anche a risolvere i problemi relativi a DNS e DHCP. Se, ad esempio, immettiamo il comando "**ipconfig / flushdns**" sarà eliminato il contenuto della cache del resolver DNS del computer.

NSLookup



```
10.211.55.1
C:\Users\vaandro>nslookup
Server: nslookup
Address: 10.211.55.1
-

```

NSlookup è un ottimo comando per **diagnosticare i problemi di risoluzione dei nomi DNS**. Infatti sarà sufficiente digitare il comando "**nslookup**" per ottenere il nome e l'indirizzo IP del server DNS predefinito del dispositivo. Partendo da qui, sarà possibile digitare i nomi host per tentare di capire se il server DNS è in grado di risolvere il nome host specificato.

Route

```
Microsoft Windows [versione 10.0.10240.0]
(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\vaandro>route print

=====
Interface
  5...00 1c 42 38 37 45 .....Parallels VMX3D Ethernet Adapter
  1.....Software Loopback Interface 1
  =====

IPv4 Tabella route

Route attive:

  Destinazione rete      Mask          Gateway        Interfaccia Metrica
-----
  0.0.0.0                0.0.0.0      10.211.55.1    30.211.55.3    25
  10.211.55.0            255.255.255.0 0.0.0.0        30.211.55.3    271
  10.211.55.1            255.255.255.255 0.0.0.0        30.211.55.3    271
  10.211.55.255         255.255.255.255 0.0.0.0        30.211.55.3    271
  127.0.0.0              255.0.0.0    0.0.0.0        127.0.0.1      331
  127.0.0.1              255.255.255.255 0.0.0.0        127.0.0.1      331
  127.255.255.255       255.255.255.255 0.0.0.0        127.0.0.1      331
  224.0.0.0              248.0.0.0    0.0.0.0        127.0.0.1      331
  255.255.255.255       255.255.255.255 0.0.0.0        127.0.0.1      331
  255.255.255.255       255.255.255.255 0.0.0.0        30.211.55.3    271

Route permanenti:
  Nessuna

IPv6 Tabella route

```

Ogni rete IP utilizza tabelle di routing per indirizzare i pacchetti da una sottorete all'altra, in questo caso il comando in questione consente di **visualizzare le tabelle di routing** del dispositivo. Per farlo è sufficiente digitare "**route print**".

Sarà inoltre possibile apportare modifiche alla tabella di routing usando alcuni comandi come "**route add**", "**route delete**" e "**route change**". Tali modifiche potranno essere persistenti o non persistenti, a seconda che si utilizzi l'opzione **-p**.

PathPing

```
Microsoft Windows [versione 10.0.10240.0]
(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\vaandro>pathping

=====
Interface
  5...00 1c 42 38 37 45 .....Parallels VMX3D Ethernet Adapter
  1.....Software Loopback Interface 1
  =====

IPv4 Tabella route

Route attive:

  Destinazione rete      Mask          Gateway        Interfaccia Metrica
-----
  0.0.0.0                0.0.0.0      10.211.55.1    30.211.55.3    25
  10.211.55.0            255.255.255.0 0.0.0.0        30.211.55.3    271
  10.211.55.1            255.255.255.255 0.0.0.0        30.211.55.3    271
  10.211.55.255         255.255.255.255 0.0.0.0        30.211.55.3    271
  127.0.0.0              255.0.0.0    0.0.0.0        127.0.0.1      331
  127.0.0.1              255.255.255.255 0.0.0.0        127.0.0.1      331
  127.255.255.255       255.255.255.255 0.0.0.0        127.0.0.1      331
  224.0.0.0              248.0.0.0    0.0.0.0        127.0.0.1      331
  255.255.255.255       255.255.255.255 0.0.0.0        127.0.0.1      331
  255.255.255.255       255.255.255.255 0.0.0.0        30.211.55.3    271

Route permanenti:
  Nessuna

IPv6 Tabella route

```



PathPing è un comando che combina i migliori aspetti delle utilità **Ping** e **Tracert**. Se seguito da un nome host, una volta terminato un processo di circa cinque minuti, si otterranno delle statistiche piuttosto dettagliate inerenti la latenza e la perdita di pacchetti.

NetDiag

NetDiag è uno dei comandi più utili perché esegue una serie completa di test utili ad individuare eventuali problemi di rete. In alcuni casi, il comando "**netdiag**" può anche tentare di risolverli automaticamente attraverso l'aggiunta del parametro **/ fix**.

Queste utilità da riga di comando sono solo una piccola parte di quelle disponibili in Windows. Nonostante alcune di esse siano state introdotte da almeno un decennio, possono essere considerate ancora oggi una risorsa molto utile per gli amministratori di rete.

