



Command Line - IMCP

created by: Nguyễn Đình Thắng

Phân biệt địa chỉ IP nội bộ vs IP công cộng và cách kiểm tra IP public

 1. Địa chỉ IP nội bộ (Private IP) là gì?

 Các dải IP nội bộ phổ biến:

 2. Địa chỉ IP công cộng (Public IP) là gì?

 3. So sánh nhanh:

 4. Cách kiểm tra IP nội bộ và IP công cộng

 Kiểm tra IP nội bộ (private IP):

 Kiểm tra IP công cộng (public IP):

Cách 1 - Dùng trình duyệt:

Cách 2 - Dùng PowerShell:

 5. Một số lưu ý quan trọng:

 Kiểm tra xem bạn đang dùng IP công cộng riêng hay CGNAT , hướng dẫn cách nhận biết.

 1. Kiểm tra IP nội bộ và IP công cộng

Bước 1: Kiểm tra IP nội bộ (trên máy tính)

Bước 2: Kiểm tra IP công cộng

 2. So sánh địa chỉ IP modem nhận được với IP công cộng

 Cách đơn giản nhất:

 Kết quả nhận biết:

 CGNAT - Là gì và ảnh hưởng gì?

 Cách khắc phục CGNAT nếu cần IP công cộng riêng:



Lệnh **ping** là gì?



Giải thích kết quả lệnh **ping** :



Các tùy chọn hữu ích của lệnh **ping** :



Khi nào
ping báo lỗi?



Ứng dụng thực tế:



2. Kiểm tra đường đi gói tin - **tracert**



Lệnh **tracert** là gì?



Kết quả mẫu của **tracert** :



Giải thích từng cột:



Các lỗi thường gặp trong **tracert** :



Một số tùy chọn mở rộng của **tracert** :



So sánh nhanh với **ping** :



Lệnh **pathping**



Lệnh **pathping** là gì?



Cách hoạt động:



Giải thích kết quả:

Cách đọc:



Tùy chọn nâng cao:



Khi nào nên dùng **pathping** ?



Lưu ý khi dùng:

Lệnh `nslookup`

 Giải thích từng dòng:

 Một số cách dùng nâng cao của `nslookup` :

-  1. Kiểm tra tên miền với DNS cụ thể
-  2. Vào chế độ tương tác để tra nhiều thứ hơn

 Khi nào nên dùng `nslookup` ?

 Lưu ý:

Lệnh `ipconfig`

 Lệnh `ipconfig` là gì?



Cú pháp cơ bản:

 Giải thích từng dòng:

 Một số lệnh mở rộng của `ipconfig` :

 Ví dụ thực tế:

 Khi nào dùng `ipconfig` ?

 `ipconfig /release` và `ipconfig /renew`

 Tổng quan về `ipconfig /release` và `ipconfig /renew`

 1. Lệnh `ipconfig /release` - Ngắt địa chỉ IP hiện tại

 Cú pháp:

 Tác dụng:

 Ví dụ:

 2. Lệnh `ipconfig /renew` - Xin cấp lại địa chỉ IP

 Cú pháp:

 Tác dụng:

 Tổng kết quá trình:

 Khi nào dùng 2 lệnh này?

 Ví dụ thực tế:

 Mẹo :

`ipconfig /flushdns`

 1. `ipconfig /flushdns` là gì?

 Cú pháp lệnh:

 2. DNS cache là gì? (Hiểu đơn giản)

 3. Khi nào cần xóa DNS cache?

4. Cách sử dụng

✨ Trên CMD (chạy quyền Admin nếu cần):

✓ 5. Lệnh liên quan hữu ích:

🎯 Tóm lại, khi nào nên dùng `ipconfig /flushdns` ?

🔌 Kiểm tra port kết nối - netstat

🧠 1. `netstat` là gì?

📘 Cú pháp cơ bản:

🔧 2. Các tham số thường dùng (nên nhớ):

✓ Ví dụ thực tế:

📌 Kiểm tra tất cả kết nối + PID:

🔧 Các trạng thái phổ biến:

🔧 Ứng dụng thực tế của `netstat`

💡 Gợi ý nâng cao:



Bảng so sánh các port mạng thường dùng

🧠 Mẹo ghi nhớ nhanh:

🔒 Port nào an toàn hơn?

Phân biệt địa chỉ IP nội bộ vs IP công cộng và cách kiểm tra IP public

🧠 1. Địa chỉ IP nội bộ (Private IP) là gì?

Đây là địa chỉ được **cấp trong mạng nội bộ**, ví dụ: mạng Wi-Fi trong nhà, mạng LAN công ty. Chỉ các thiết bị trong cùng mạng mới thấy **nhau** qua IP này.

Các dải IP nội bộ phổ biến:

Dải IP	Ghi chú
192.168.0.0 – 192.168.255.255	Phổ biến nhất trong mạng gia đình
10.0.0.0 – 10.255.255.255	Dùng nhiều ở doanh nghiệp lớn
172.16.0.0 – 172.31.255.255	Ít gặp hơn, vẫn là private

👉 Không thể truy cập từ ngoài Internet đến IP nội bộ nếu không cấu hình NAT.

2. Địa chỉ IP công cộng (Public IP) là gì?

- Là địa chỉ IP được ISP (nhà mạng như Viettel, FPT, VNPT...) cấp ra Internet.
- Dùng để giao tiếp với Internet – ví dụ truy cập web, game, video call...
- Nếu mở port, người ngoài có thể truy cập máy bạn qua IP này (nếu NAT).

3. So sánh nhanh:

Tiêu chí	IP nội bộ (Private)	IP công cộng (Public)
Tầm hoạt động	Trong mạng LAN	Toàn Internet
Có thể truy cập từ ngoài?	❌ Không	✅ Có (nếu cấu hình đúng)
Cấp bởi	Modem/router (DHCP)	ISP (nhà mạng)
Dải IP	192.168.x.x, 10.x.x.x...	Bất kỳ IP ngoài các dải private
Có thể trùng nhau?	✅ Có (giữa các mạng khác nhau)	❌ Không (phải duy nhất toàn cầu)

4. Cách kiểm tra IP nội bộ và IP công cộng

✓ Kiểm tra IP nội bộ (private IP):

Chạy trong Command Prompt hoặc PowerShell:

```
ipconfig
```

👉 Dò phần:

```
IPv4 Address. . . . : 192.168.1.5
```

✓ Kiểm tra IP công cộng (public IP):

Bạn không thể thấy IP public bằng `ipconfig`, vì nó là của router. Hãy dùng trang web:

Cách 1 – Dùng trình duyệt:

Truy cập:

- <https://whatismyipaddress.com>
- <https://ipinfo.io>
- <https://www.myip.com>

Sẽ hiển thị:

```
Your IP Address: 113.161.98.75  
ISP: Viettel
```

Location: Ho Chi Minh, Vietnam

Cách 2 – Dùng PowerShell:

```
(Invoke-WebRequest -uri "https://api.ipify.org").Content
```

👉 Trả về IP công cộng.

5. Một số lưu ý quan trọng:

- Nếu bạn dùng **CGNAT (Carrier-grade NAT)**, bạn sẽ không được cấp IP công cộng riêng → không thể mở port hoặc truy cập từ xa.
- Nếu cần **truy cập camera/NAS từ xa**, bạn phải có **IP public tĩnh** hoặc dùng **dịch vụ DDNS**.

Kiểm tra xem bạn đang dùng IP công cộng riêng hay CGNAT , hướng dẫn cách nhận biết.

Việc xác định xem bạn đang dùng **IP công cộng riêng (public IP trực tiếp)** hay đang bị **CGNAT (Carrier-Grade NAT)** là rất quan trọng nếu bạn cần:

- Mở port (camera, game, remote desktop...)

- Cài server tại nhà
- Truy cập thiết bị từ xa qua mạng ngoài

Dưới đây là **cách kiểm tra và nhận biết chính xác**.

1. Kiểm tra IP nội bộ và IP công cộng

Bước 1: Kiểm tra IP nội bộ (trên máy tính)

Mở **CMD** hoặc **PowerShell**, gõ:

```
ipconfig
```

➡ Ghi lại dòng:

```
IPv4 Address. . . . : 192.168.x.x (hoặc 10.x.x.x)  
Default Gateway . . : 192.168.1.1
```

Bước 2: Kiểm tra IP công cộng

Truy cập 1 trong các trang sau từ trình duyệt:

- <https://whatismyipaddress.com>
- <https://www.myip.com>
- <https://ipinfo.io>

➡ Ghi lại địa chỉ IP mà website hiển thị.

2. So sánh địa chỉ IP modem nhận được với IP công cộng

✓ Cách đơn giản nhất:

1. Truy cập vào trang cài đặt modem/router (thường là: `192.168.1.1`)
2. Đăng nhập (user/pass mặc định có thể là `admin/admin`)
3. Tìm phần:
 - WAN Info
 - Internet Status
 - WAN IP Address / Internet IP

➡ So sánh IP này với IP bạn thấy từ website bên trên.

📌 Kết quả nhận biết:

So sánh	Ý nghĩa
IP modem giống IP công cộng trên web	✓ Bạn có IP công cộng riêng (có thể mở port)
IP modem là 10.x.x.x hoặc 100.64.x.x (nhưng web hiển thị IP khác)	✗ Bạn đang dùng CGNAT
IP modem là 192.168.x.x	Bạn đang NAT nhiều lớp (double NAT) → cũng là CGNAT hoặc bị router trung gian

🧠 CGNAT – Là gì và ảnh hưởng gì?

- CGNAT là kỹ thuật mà nhà mạng **chia sẻ 1 IP công cộng cho nhiều khách hàng** → tiết kiệm IP.
- Bạn sẽ **không có quyền mở port**, và **không thể truy cập từ xa về mạng nhà**.
- Phổ biến ở mạng di động (4G), Internet cáp quang phổ thông Viettel, VNPT, FPT.

Cách khắc phục CGNAT nếu cần IP công cộng riêng:

Cách	Mô tả
Gọi tổng đài nhà mạng	Yêu cầu cấp IP công cộng tĩnh hoặc động
Dùng dịch vụ DDNS + mở port (nếu có IP public)	Truy cập từ xa qua tên miền
Dùng VPN hoặc Cloudflare Tunnel	Vượt qua giới hạn CGNAT, dùng trong server, camera
Nâng cấp gói doanh nghiệp	Một số gói cáp quang doanh nghiệp có IP công cộng riêng mặc định

Bạn có thể gửi mình:

- Ảnh chụp phần WAN IP trong modem
- IP trên <https://whatismyipaddress.com>

→ Mình sẽ xác định giúp bạn có đang bị CGNAT không. Bạn muốn mình hướng dẫn truy cập vào modem không?



Lệnh **ping** là gì?

Lệnh **ping** được dùng để kiểm tra xem máy tính của bạn có thể giao tiếp với một thiết bị mạng khác hay không (ví dụ: website, server, router...).

Nó hoạt động bằng cách:

1. Gửi các gói dữ liệu nhỏ (gọi là ICMP Echo Request).
2. Thiết bị đích nhận được thì gửi lại (ICMP Echo Reply).
3. Máy bạn đo thời gian đi-về của gói tin

```
ping <địa_chỉ_IP_hoặc_tên_miền>
```

```
ping google.com
```

```
ping 8.8.8.8
```



Giải thích kết quả lệnh **ping** :

Pinging google.com [142.250.196.110] with 32 bytes of data:

Reply from 142.250.196.110: bytes=32 time=15ms TTL=113

Reply from 142.250.196.110: bytes=32 time=17ms TTL=113

Reply from 142.250.196.110: bytes=32 time=14ms TTL=113

Reply from 142.250.196.110: bytes=32 time=15ms TTL=113

Ping statistics for 142.250.196.110:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 14ms, Maximum = 17ms, Average = 15ms

Chi tiết từng phần:

- **Reply from...** : Nhận được phản hồi → kết nối OK.
- **bytes=32** : Mỗi gói gửi có 32 byte.
- **time=15ms** : Mất 15 milli giây để đi và về → càng thấp càng tốt.
- **TTL=113** : Time to Live (giới hạn số hop - chỉ mang tính kỹ thuật sâu hơn).
- **Lost = 0** : Không mất gói nào → kết nối ổn định.



Các tùy chọn hữu ích của lệnh **ping** :

Tùy chọn	Ý nghĩa
-t	Ping liên tục (dừng bằng Ctrl + C)
-n <số>	Số lần ping cụ thể (mặc định là 4)
-l <size>	Kích thước gói tin gửi đi (mặc định là 32 byte)
-4 hoặc -6	Chọn IPv4 hoặc IPv6

```
ping -t 8.8.8.8      :: Ping liên tục Google DNS
ping -n 10 google.com  :: Ping 10 lần
ping -l 1000 google.com  :: Gửi gói 1000 byte để kiểm tra tốc độ mạng
```

Khi nào **ping** báo lỗi?

Request timed out.
Destination host unreachable.
Ping request could not find host.

- **Request timed out.** → Gói gửi đi không được trả về → Mất kết nối hoặc bị chặn.
- **Destination host unreachable.** → Không tìm thấy đường đến IP/host.
- **Could not find host** → Sai tên miền hoặc lỗi DNS.

Ứng dụng thực tế:

- Kiểm tra xem có kết nối internet không (`ping 8.8.8.8`)
- Kiểm tra server game có phản hồi không.
- Kiểm tra độ ổn định mạng (ping nhiều lần → xem có mất gói, độ trễ cao không).



2. Kiểm tra đường đi gói tin - `tracert`



Lệnh `tracert` là gì?

- `tracert` (trên Windows, trong Linux thì là `traceroute`) dùng để **hiển thị từng bước (hop)** mà một gói tin phải đi qua để đến đích.
- Nó giúp **xác định chỗ nào trong mạng bị chậm, nghẽn, hoặc không đi được**.

```
tracert <tên_miền_hoặc_địa_chỉ_IP>
```

```
tracert google.com
```

```
tracert 8.8.8.8
```

- Cho biết gói tin đi qua các router nào đến đích.
- Xem bị chậm/mất gói ở đâu (hop nào).



Kết quả mẫu của **tracert** :

Tracing route to google.com [142.250.196.78] over a maximum of 30 hops:

```

1  1 ms  1 ms  1 ms  192.168.1.1    ← Router nhà bạn
2  10 ms  9 ms  11 ms  10.20.30.1      ← Thiết bị ISP (Viettel, FPT,...)
3  15 ms  14 ms  13 ms  203.113.xx.xx   ← Node trung gian
4  22 ms  20 ms  21 ms  72.14.234.xxx   ← Google server
5  24 ms  23 ms  22 ms  142.250.196.78  ← Địa chỉ đích

```

Trace complete.



Giải thích từng cột:

Cột	Ý nghĩa
Số đầu dòng	Số thứ tự hop (bước nhảy)
3 thời gian (ms)	Thời gian phản hồi từ thiết bị đó trong 3 lần gửi
Địa chỉ IP hoặc tên host	Là thiết bị mà gói tin đi qua

Mỗi "hop" là một router hoặc thiết bị trung gian mà gói tin đi qua.

Ý nghĩa thực tế:

- Xem **đường đi gói tin** từ máy bạn đến server.
- Xác định **nút mạng nào gây chậm trễ hoặc mất gói**.
- Biết server đích đang ở **quốc gia nào, mạng nào**.
- Nếu mạng nội bộ OK nhưng từ hop thứ 2 trở đi chậm → lỗi phía nhà mạng.
- Nếu **tracert** bị dừng giữa chừng → có thể gói bị chặn (firewall/NAT).

Các lỗi thường gặp trong **tracert** :

Dòng hiển thị	Nguyên nhân
Request timed out.	Thiết bị trung gian không trả lời ICMP (bị chặn, firewall)
* * *	Giống trên - không phản hồi
Không đi hết 30 hop	Bị chặn, hoặc mạng không có đường đến

Một số tùy chọn mở rộng của **tracert** :

Tùy chọn	Ý nghĩa
----------	---------

<code>-d</code>	Không phân giải tên miền (tăng tốc độ)
<code>-h <số></code>	Giới hạn số hop (mặc định là 30)
<code>-w <ms></code>	Thời gian chờ phản hồi (mặc định 4000ms = 4s)

tracert -d google.com :: Không phân giải DNS → nhanh hơn
tracert -h 15 8.8.8.8 :: Dừng sau 15 hop
tracert -w 2000 google.com :: Giảm thời gian chờ mỗi hop xuống 2s

So sánh nhanh với `ping` :

<code>ping</code>	<code>tracert</code>
Kiểm tra tổng thể có kết nối không	Kiểm tra từng bước đi qua
Không biết đi qua router nào	Biết rõ từng hop đi qua
Thích hợp kiểm tra mất mạng	Thích hợp tìm vị trí lỗi/chậm



Lệnh `pathping`



Lệnh `pathping` là gì?

`pathping` là tổ hợp giữa `ping` và `tracert`, dùng để:

- **Xác định đường đi của gói tin** từ máy bạn đến một đích (giống `tracert`).
- **Đo lường tỉ lệ mất gói (packet loss)** ở từng bước (hop).
- **Xác định router hoặc mạng nào gây chậm hoặc mất gói.**

```
pathping <địa_chỉ_IP hoặc tên_miền>
pathping google.com
pathping 8.8.8.8
```

Cách hoạt động:

1. **Giai đoạn 1:** Liệt kê các hop giống như `tracert`.
2. **Giai đoạn 2:** Gửi nhiều gói tin tới từng hop trong khoảng **25-30 giây** để đo **độ trễ và mất gói**.
3. Sau đó, nó **phân tích kết quả chi tiết**, giúp bạn biết chỗ nào bị lỗi thật sự.



Ví dụ kết quả `pathping` :

```
Tracing route to google.com [142.250.196.110] over a maximum of 30 hops:
 0 My-PC [192.168.1.10]
 1 192.168.1.1
 2 10.20.30.1
 3 203.113.xx.xx
```

```
4 72.14.xxx.xxx
5 142.250.196.110
```

Computing statistics for 125 seconds...

```
      Source to Here  This Node/Link
Hop  RTT  Lost/Sent = Pct  Lost/Sent = Pct  Address
0      0/ 100 = 0%  NA              My-PC
1  1ms   0/ 100 = 0%   0/100 = 0%   192.168.1.1
2 10ms   0/ 100 = 0%   0/100 = 0%   10.20.30.1
3 14ms   3/ 100 = 3%   3/100 = 3%   203.113.xx.xx
4 23ms   0/ 100 = 0%   0/100 = 0%   72.14.xxx.xxx
5 25ms   0/ 100 = 0%   0/100 = 0%   142.250.196.110
```

Giải thích kết quả:

Cột	Ý nghĩa
Hop	Số thứ tự của điểm mạng (router, server...)
RTT (Round Trip Time)	Thời gian đi và về của gói tin
Lost/Sent = Pct (Source to Here)	Tỷ lệ mất gói từ máy bạn đến hop đó
Lost/Sent = Pct (This Node/Link)	Tỷ lệ mất gói xảy ra tại chính node đó

Cách đọc:

- Nếu cột "This Node/Link" > 0%, thì **node đó là nguyên nhân gây mất gói**.
- Nếu cột này = 0%, nhưng "Source to Here" tăng dần → **node trước đó bị nghẽn**.

Tùy chọn nâng cao:

Tùy chọn	Ý nghĩa
<code>-n</code>	Không phân giải DNS (hiển thị IP, nhanh hơn)
<code>-h <số></code>	Giới hạn số hop
<code>-w <ms></code>	Đặt thời gian chờ phản hồi

pathping -n google.com :: Không phân giải tên miền
pathping -n -h 10 8.8.8.8 :: Giới hạn tối đa 10 hop

Khi nào nên dùng `pathping` ?

- Khi bạn thấy **lag hoặc mất kết nối bất thường**, nhưng `ping` vẫn trả về.
- Khi bạn nghi ngờ **mạng chậm do một hop nào đó**, nhất là trong mạng nội bộ hoặc mạng của nhà mạng.
- Khi cần **xác định chính xác router gây mất gói**.

Lưu ý khi dùng:

- Lệnh này **mất thời gian khoảng 2-3 phút** để hoàn tất → đừng ngắt giữa chừng.
- Một số router hoặc ISP **chặn phản hồi ICMP**, nên có thể hiện `Request timed out` nhưng không phải lúc nào cũng là lỗi.



Lệnh nslookup

nslookup (Name Server Lookup) được dùng để:

- Kiểm tra địa chỉ IP của một tên miền.
- Xem máy tính đang dùng DNS nào để phân giải tên miền.
- Chẩn đoán các sự cố liên quan đến DNS, như: web/game không vào được do lỗi phân giải tên miền.

```
nslookup google.com
```

```
Server: dns.google
```

```
Address: 8.8.8.8
```

```
Non-authoritative answer:
```

```
Name: google.com
```

```
Addresses: 142.250.196.14
```

```
2404:6800:4003:c1a::8a
```



Giải thích từng dòng:

Dòng	Ý nghĩa
------	---------

Server	Tên DNS server đang được dùng để phân giải
Address	IP của DNS server
Non-authoritative answer	Kết quả từ DNS cache hoặc trung gian, không phải máy chủ gốc
Name	Tên miền bạn tra
Addresses	IP IPv4 hoặc IPv6 tương ứng với tên miền

Một số cách dùng nâng cao của **nslookup** :

1. Kiểm tra tên miền với DNS cụ thể

```
nslookup google.com 8.8.8.8
```

→ Dùng DNS của Google để phân giải, bỏ qua DNS mặc định của máy bạn.

2. Vào chế độ tương tác để tra nhiều thứ hơn

Gõ **nslookup** rồi Enter → vào chế độ tương tác:

```
> nslookup
> set type=A
> google.com
```

Bạn có thể đổi loại truy vấn để tra nhiều thông tin hơn:

Lệnh	Ý nghĩa
set type=A	Truy vấn IP (IPv4)

<code>set type=AAAA</code>	Truy vấn IPv6
<code>set type=MX</code>	Xem mail server của tên miền
<code>set type=NS</code>	Xem name server của tên miền
<code>set type=TXT</code>	Xem bản ghi TXT (ví dụ SPF, Google verify...)

3.

Xem bản ghi mail server của tên miền

```
nslookup -type=mx gmail.com
```

Khi nào nên dùng `nslookup` ?

- Khi truy cập web/game bị lỗi tên miền không tìm thấy.
- Khi nghi ngờ DNS phân giải sai hoặc chậm.
- Khi cần xác định **IP thật của server** (tránh fake DNS, lừa đảo).
- Khi cấu hình **mail server, hosting, domain**.

Lưu ý:

- Nếu bạn gõ `nslookup <tên miền>` mà không ra IP → máy bạn đang **lỗi DNS** hoặc tên miền bị **trò sai**.
- Có thể thử với DNS khác như Google (8.8.8.8) hoặc Cloudflare (1.1.1.1) để so sánh.



Lệnh `ipconfig`



Lệnh `ipconfig` là gì?

- `ipconfig` (*IP Configuration*) được dùng để xem thông tin cấu hình mạng của máy tính Windows, như:
 - Địa chỉ IP
 - Địa chỉ Gateway (modem/router)
 - Địa chỉ DNS
 - Mạng nào đang được kết nối



Cú pháp cơ bản:

```
ipconfig
```



Kết quả mẫu:

```
Wireless LAN adapter Wi-Fi:
```

```
Connection-specific DNS Suffix . : viettel.vn
```

```
IPv4 Address. . . . . : 192.168.1.5
```


Subnet Mask : 255.255.255.0
Default Gateway : 192.168.1.1

Giải thích từng dòng:

Dòng	Ý nghĩa
Wireless LAN adapter Wi-Fi	Tên card mạng (ở đây là card Wi-Fi)
Connection-specific DNS Suffix	Tên miền nội bộ được gán bởi mạng
IPv4 Address	Địa chỉ IP nội bộ của máy bạn trên mạng LAN
Subnet Mask	Mặt nạ mạng, thường là 255.255.255.0 trong mạng gia đình
Default Gateway	Địa chỉ IP của modem/router – cổng ra Internet

Một số lệnh mở rộng của **ipconfig** :

Lệnh	Tác dụng
ipconfig /all	Xem tất cả thông tin chi tiết (bao gồm DNS, MAC address, DHCP...)
ipconfig /release	Ngắt IP hiện tại (thường dùng khi reset mạng)
ipconfig /renew	Xin cấp IP mới từ DHCP (thường dùng sau khi /release)
ipconfig /flushdns	Xoá cache DNS cũ – dùng khi web bị lỗi tên miền

Ví dụ thực tế:

```
ipconfig /all
```

Sẽ hiển thị thêm:

- MAC Address (Physical Address)
- DNS Server đang dùng
- DHCP Enabled (máy có tự xin IP hay không)
- Lease Obtained/Expires (thời gian cấp phát IP)

2. Sửa lỗi khi không vào được mạng:

```
ipconfig /release  
ipconfig /renew
```

→ Dùng khi IP bị trùng hoặc không được cấp.

3. Sửa lỗi không vào được website:

```
ipconfig /flushdns
```

→ Xoá bộ nhớ DNS cache, giúp máy tính phân giải tên miền lại từ đầu.

 **Khi nào dùng `ipconfig` ?**

- Khi bạn **muốn biết địa chỉ IP hiện tại** của máy.
- Khi bạn cần xác định **router/gateway** để truy cập cài đặt.
- Khi cấu hình mạng, NAT, forwarding, hoặc kiểm tra lỗi IP.
- Khi bị **xung đột IP**, không vào được mạng, mạng chậm hoặc **DNS lỗi**.



ipconfig /release

và

ipconfig /renew



Tổng quan về **ipconfig /release** và **ipconfig /renew**

Hai lệnh này dùng để:

- Ngắt kết nối IP hiện tại (**release**)
- Xin cấp lại địa chỉ IP mới (**renew**)
- Thường dùng để **sửa lỗi mạng, xung đột IP, hoặc mất kết nối**



1. Lệnh **ipconfig /release** – Ngắt địa chỉ IP hiện tại



Cú pháp:

```
ipconfig /release
```

Tác dụng:

- Bỏ địa chỉ IP hiện tại mà card mạng đang dùng.
- Máy sẽ mất kết nối Internet tạm thời (**IP = 0.0.0.0**).
- Dùng khi bạn muốn "reset" IP do lỗi hoặc xung đột.

Ví dụ:

Ethernet adapter Wi-Fi:

```
Connection-specific DNS Suffix . :  
IPv4 Address. . . . . : 0.0.0.0  
Subnet Mask . . . . . : 0.0.0.0
```

2. Lệnh `ipconfig /renew` – Xin cấp lại địa chỉ IP

Cú pháp:

```
ipconfig /renew
```

Tác dụng:

- Gửi yêu cầu tới modem/router (DHCP server) để **xin cấp IP mới**.
- Máy tính nhận lại:
 - IP mới (nếu có)
 - Subnet mask

- Default gateway
- DNS server

👉 Thường dùng ngay sau `/release` để khôi phục kết nối.

Tổng kết quá trình:

Bước	Lệnh	Mô tả
1	<code>ipconfig /release</code>	Bỏ IP đang dùng
2	<code>ipconfig /renew</code>	Xin IP mới từ DHCP

Khi nào dùng 2 lệnh này?

- Mạng bị lỗi, **không có Internet**, hoặc thông báo “Unidentified Network”
- Bị **xung đột IP** (2 thiết bị dùng chung IP)
- Modem/router vừa khởi động lại → máy chưa xin được IP
- Sau khi thay đổi cài đặt DHCP trong router
- Chuyển sang mạng mới mà không kết nối được

Ví dụ thực tế:

```
ipconfig /release  
ipconfig /renew
```

Kết quả: máy bạn sẽ được gán lại IP từ modem, thường là kiểu:

IPv4 Address. . . . : 192.168.1.5
Default Gateway . . : 192.168.1.1



Mẹo :

- Bạn cũng có thể dùng thêm:

```
ipconfig /flushdns
```

→ Để xóa cache DNS cũ, kết hợp giúp sửa lỗi **web/game không truy cập được**.



ipconfig /flushdns



1. **ipconfig /flushdns** là gì?

- Đây là lệnh dùng để **xóa bộ nhớ đệm DNS (DNS cache)** trên máy tính.

- DNS cache lưu lại tên miền và địa chỉ IP tương ứng mà bạn đã truy cập, giúp **tăng tốc độ truy cập** lần sau.
- Tuy nhiên, nếu thông tin DNS bị **lỗi hoặc cũ**, bạn có thể **không truy cập được website** dù mạng vẫn bình thường.

Cú pháp lệnh:

```
ipconfig /flushdns
```

Sau khi chạy, bạn sẽ thấy dòng thông báo:

```
Successfully flushed the DNS Resolver Cache.
```

2. DNS cache là gì? (Hiểu đơn giản)

Tên miền (bạn nhập)	Địa chỉ IP thật (DNS trả về)
<code>www.google.com</code>	<code>142.250.190.68</code>
<code>www.facebook.com</code>	<code>157.240.22.35</code>

➡ Máy tính sẽ **lưu lại những thông tin này tạm thời**, để không phải hỏi lại DNS server mỗi lần.

3. Khi nào cần xóa DNS cache?

Tình huống	Giải thích
Không vào được website (nhưng người khác vào được)	Có thể bạn đang lưu DNS lỗi

Web đã đổi IP host mới nhưng vẫn load IP cũ	DNS cũ chưa cập nhật
Đang test tên miền mới / cấu hình lại domain	Cần xóa DNS cũ để thấy kết quả mới
Lỗi SSL không rõ nguyên nhân	Có thể do DNS cache lỗi gây ra

4. Cách sử dụng

🌟 Trên CMD (chạy quyền Admin nếu cần):

```
ipconfig /flushdns
```

➡ Kết quả:

```
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
```

✅ 5. Lệnh liên quan hữu ích:

Lệnh	Tác dụng
<code>ipconfig /displaydns</code>	Xem danh sách DNS đang được lưu
<code>ipconfig /flushdns</code>	Xóa toàn bộ DNS đang lưu
<code>nslookup tenmien.com</code>	Kiểm tra tên miền hiện trỏ về IP nào
<code>ipconfig /registerdns</code>	Đăng ký lại DNS của máy với mạng nội bộ (ít dùng)

 Tóm lại, khi nào nên dùng `ipconfig /flushdns` ?

- Website không truy cập được mà mạng vẫn bình thường

- Web mới mua hoặc mới thay IP, nhưng máy bạn vẫn truy IP cũ
- Chuyển hosting, sửa domain, dùng VPN hoặc proxy xong bị lỗi web
- Sửa lỗi không rõ ràng liên quan DNS

Kiểm tra port kết nối – netstat

1. **netstat** là gì?

- **netstat** viết tắt của **Network Statistics**
- Là lệnh dùng để:
 - Xem **các cổng (port)** mà máy đang dùng để **giao tiếp**
 - Kiểm tra **IP và cổng** của các **kết nối đến/đi**
 - Xem ứng dụng nào đang sử dụng cổng nào
 - Hữu ích để kiểm tra **kết nối ẩn, port đang mở, phần mềm độc hại, dịch vụ đang lắng nghe**

Cú pháp cơ bản:

```
netstat
```

Hiển thị các kết nối TCP đang hoạt động.

2. Các tham số thường dùng (nên nhớ):

Lệnh	Tác dụng
<code>netstat -a</code>	Hiển thị tất cả kết nối và cổng đang "lắng nghe" (listening)
<code>netstat -n</code>	Hiển thị IP & port dưới dạng số (không phân giải tên miền) – nhanh hơn
<code>netstat -o</code>	Hiển thị PID (Process ID) của tiến trình đang dùng kết nối
<code>netstat -an</code>	Kết hợp: tất cả kết nối + dạng số
<code>netstat -ano</code>	Chi tiết nhất: tất cả + IP/port + PID
<code>netstat -b</code>	Hiển thị tên file .exe dùng kết nối đó (cần quyền admin)

Ví dụ thực tế:

Kiểm tra tất cả kết nối + PID:

```
netstat -ano
```

Kết quả ví dụ:

```
Proto Local Address      Foreign Address    State       PID
TCP    192.168.1.5:49756  172.217.24.174:443 ESTABLISHED 3400
```

Ý nghĩa:

Cột	Ý nghĩa
Proto	Giao thức (TCP/UDP)
Local Address	IP + Port máy bạn đang dùng
Foreign Address	IP + Port của máy bên kia (server)

State	Trạng thái (ESTABLISHED, LISTENING, TIME_WAIT...)
PID	Mã tiến trình đang dùng cổng đó

👉 Bạn có thể tìm xem PID 3400 là chương trình gì bằng:

```
tasklist | find "3400"
```

Các trạng thái phổ biến:

Trạng thái	Giải thích
LISTENING	Đang chờ kết nối (dịch vụ lắng nghe port)
ESTABLISHED	Đã kết nối thành công
TIME_WAIT	Đang đóng kết nối
CLOSE_WAIT	Chờ đóng kết nối từ client
SYN_SENT	Đang gửi yêu cầu kết nối

Ứng dụng thực tế của **netstat**

Mục đích	Lệnh gợi ý
Kiểm tra có phần mềm lạ dùng port không	<code>netstat -ano</code> + <code>tasklist</code>
Kiểm tra port camera/server có đang mở không	<code>`netstat -an</code>
Kiểm tra có kết nối ra ngoài không rõ nguồn	<code>netstat -b</code>
Kiểm tra xem port có đang "listening"	<code>netstat -a</code>

Gợi ý nâng cao:

- Dùng kết hợp với PowerShell:

```
netstat -ano | findstr :80
```

- Dùng **TCPView** của Sysinternals (giao diện trực quan hơn netstat).



Bảng so sánh các port mạng thường dùng

Dịch vụ	Port (TCP/UDP)	Giao thức	Chức năng chính	Ghi chú
HTTP	80 (TCP)	TCP	Truy cập website không mã hóa	Dễ bị chặn/nghe lén
HTTPS	443 (TCP)	TCP	Truy cập website mã hóa SSL/TLS	An toàn, phổ biến nhất hiện nay
FTP (Control)	21 (TCP)	TCP	Truyền file, điều khiển phiên FTP	Không mã hóa, thường dùng cho máy chủ file
FTP (Data)	20 (TCP)	TCP	Truyền dữ liệu file (FTP active mode)	Phụ thuộc vào chế độ truyền của FTP

SSH	22 (TCP)	TCP	Quản trị server từ xa an toàn (mã hóa)	Dùng trong Linux, lập trình, server
Telnet	23 (TCP)	TCP	Quản trị từ xa không mã hóa	Đã lỗi thời, dễ bị tấn công
SMTP	25 (TCP)	TCP	Gửi email (Simple Mail Transfer Protocol)	Dùng cho máy chủ gửi mail
DNS	53 (UDP/TCP)	UDP/TCP	Phân giải tên miền (domain → IP)	UDP nhanh hơn, TCP dùng khi dữ liệu lớn
POP3	110 (TCP)	TCP	Nhận email từ server (không mã hóa)	Cũ, thay dần bằng IMAP
IMAP	143 (TCP)	TCP	Nhận email (hỗ trợ đồng bộ, thư mục)	Thay thế POP3
RDP	3389 (TCP)	TCP	Remote Desktop (Windows)	Cần mở port để truy cập từ xa
MySQL	3306 (TCP)	TCP	Kết nối đến cơ sở dữ liệu MySQL	Thường giới hạn trong mạng nội bộ
MSSQL Server	1433 (TCP)	TCP	Cơ sở dữ liệu Microsoft SQL Server	Mặc định cho SQL Server

Mẹo ghi nhớ nhanh:

- **80 / 443** → Web (HTTP, HTTPS)
- **21 / 20** → FTP (file)
- **22** → SSH (secure shell)

- **53** → DNS
 - **25 / 110 / 143** → Email
 - **3389** → Remote Desktop
-



Port nào an toàn hơn?

Port	Có mã hóa?	An toàn?
443 (HTTPS)	✓ Có SSL/TLS	✓
22 (SSH)	✓ Mã hóa	✓
21 (FTP)	✗ Không mã hóa	✗
23 (Telnet)	✗ Không mã hóa	✗