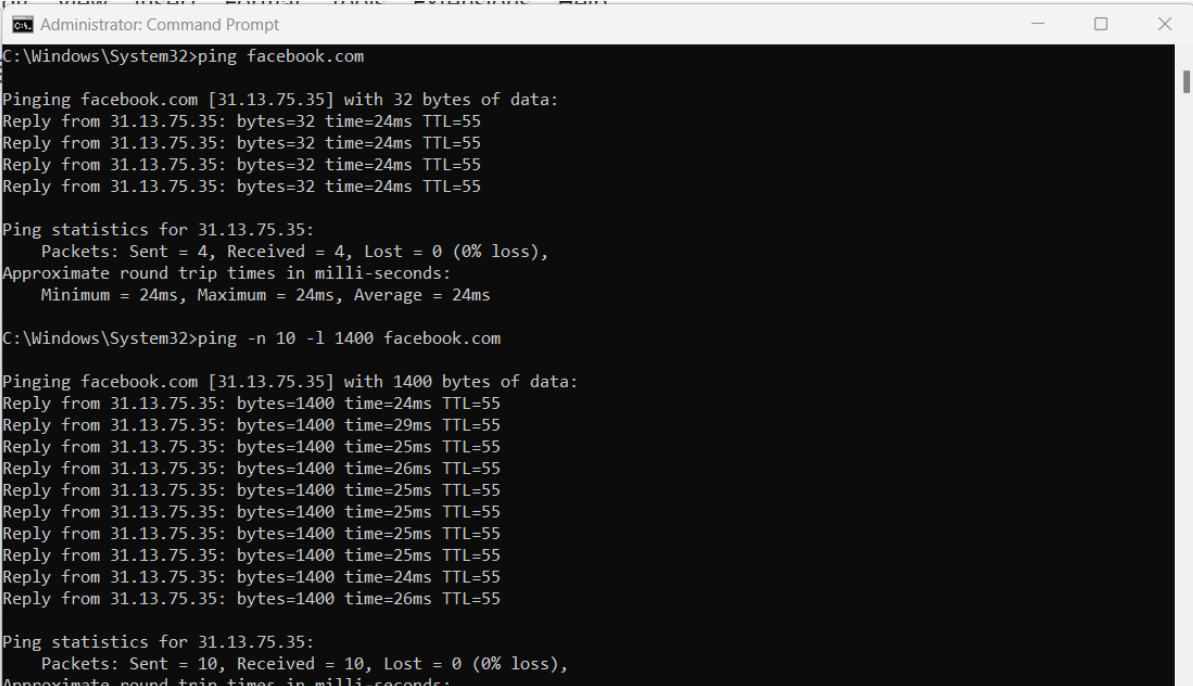


# SỬ DỤNG CÁC CÔNG CỤ TRONG WINDOWS ĐỂ PHÂN TÍCH , KIỂM TRA NETWORK

## 1. Lệnh Ping

**ping** được sử dụng để kiểm tra kết nối mạng giữa máy tính của bạn và một máy chủ hoặc địa chỉ IP khác trên mạng. Khi bạn chạy lệnh ping, nó gửi các gói tin ICMP (Internet Control Message Protocol) đến đích và chờ nhận lại các gói tin phản hồi từ đích. Mục đích chính của lệnh ping là đo lường thời gian phản hồi (latency) giữa hai máy tính và kiểm tra xem liệu có thể kết nối thành công với đích hay không.

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the execution of two ping commands. The first command is "ping facebook.com", which returns four replies from IP 31.13.75.35 with 32 bytes of data, each taking 24ms and having a TTL of 55. The statistics show 4 packets sent and received with 0% loss and an average round trip time of 24ms. The second command is "ping -n 10 -l 1400 facebook.com", which returns ten replies from the same IP with 1400 bytes of data. The round trip times vary slightly (24ms to 29ms), and the statistics show 10 packets sent and received with 0% loss.

```
C:\Windows\System32>ping facebook.com

Pinging facebook.com [31.13.75.35] with 32 bytes of data:
Reply from 31.13.75.35: bytes=32 time=24ms TTL=55
Reply from 31.13.75.35: bytes=32 time=24ms TTL=55
Reply from 31.13.75.35: bytes=32 time=24ms TTL=55
Reply from 31.13.75.35: bytes=32 time=24ms TTL=55

Ping statistics for 31.13.75.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 24ms, Average = 24ms

C:\Windows\System32>ping -n 10 -l 1400 facebook.com

Pinging facebook.com [31.13.75.35] with 1400 bytes of data:
Reply from 31.13.75.35: bytes=1400 time=24ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=29ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=25ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=26ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=25ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=25ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=25ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=25ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=24ms TTL=55
Reply from 31.13.75.35: bytes=1400 time=26ms TTL=55

Ping statistics for 31.13.75.35:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

## 2. Lệnh Telnet

**telnet facebook.com 80** sẽ thử kết nối tới máy chủ facebook.com thông qua giao thức Telnet trên cổng 80. Cổng 80 là cổng mặc định dành cho giao thức HTTP (Hypertext Transfer Protocol) được sử dụng để truyền tải dữ liệu web qua mạng.

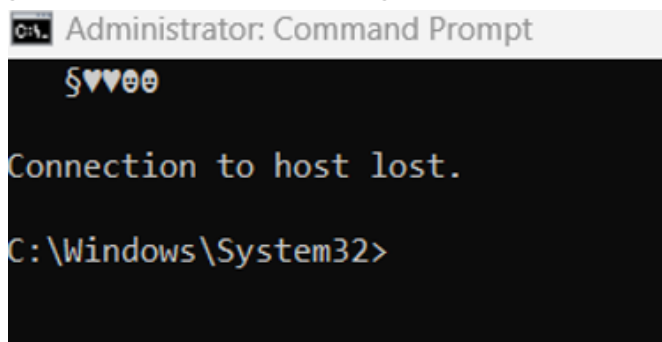
```

HTTP/1.1 400 Bad Request
Content-Type: text/html; charset=utf-8
Date: Sat, 20 May 2023 02:50:00 GMT
Connection: close
Content-Length: 2959

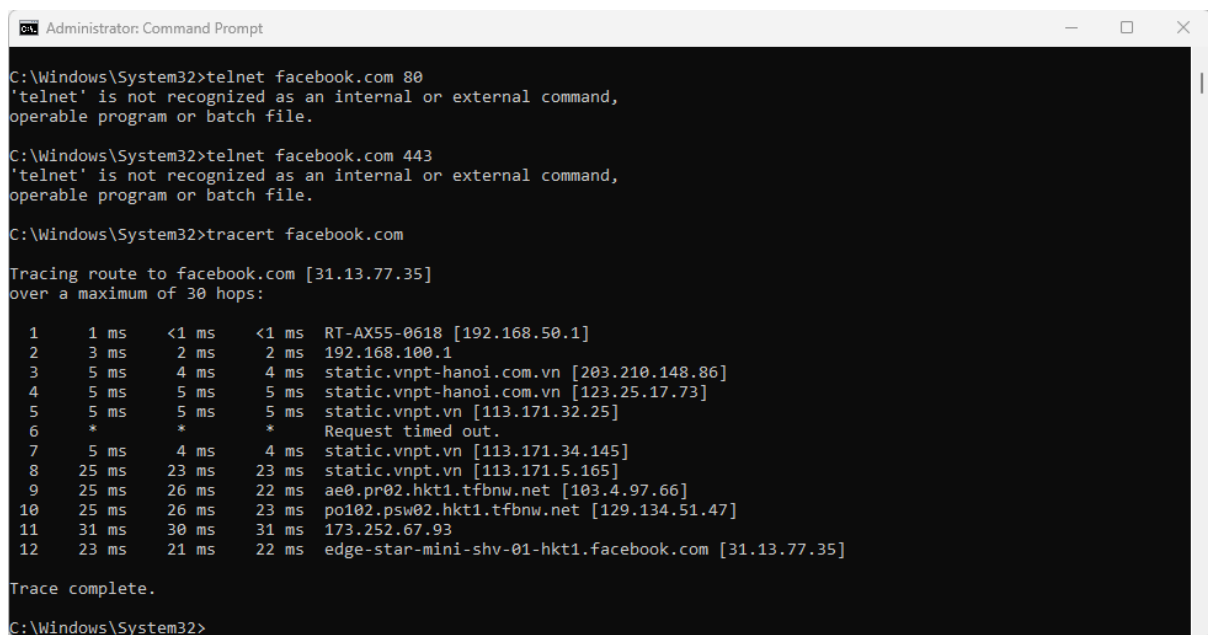
<!DOCTYPE html>
<html lang="en" id="facebook">
  <head>
    <title>Facebook | Error</title>
    <meta charset="utf-8">
    <meta http-equiv="cache-control" content="no-store">
    <meta http-equiv="cache-control" content="no-cache">
    <meta http-equiv="expires" content="-1">
    <meta http-equiv="pragma" content="no-cache">
    <meta name="robots" content="noindex,nofollow">
    <style>
      html, body {
        color: #141823;
        background-color: #e9eae4;
        font-family: Helvetica, Lucida Grande, Arial,
          Tahoma, Verdana, sans-serif;
        margin: 0;
        padding: 0;
        text-align: center;
      }
      #header {
        height: 30px;
        padding-bottom: 10px;
        padding-top: 10px;
        text-align: center;
      }
      #icon {
        width: 30px;
      }
      h1 {
        font-size: 18px;
      }
      p {
        font-size: 13px;
      }
      #footer {
        border-top: 1px solid #ddd;

```

**telnet facebook.com 443** sẽ thử kết nối tới máy chủ facebook.com thông qua giao thức Telnet trên cổng 443.



### 3. Tracert



**tracert facebook.com** sẽ hiển thị một danh sách các điểm dừng trên đường truyền từ máy tính của em tới máy chủ Facebook. Các điểm dừng này thường là các địa chỉ IP của các router hoặc các nút mạng trên đường truyền. Kết quả thường bao gồm số TTL (Time to Live) của gói tin, địa chỉ IP của điểm dừng và thời gian phản hồi từ điểm dừng đó.

```
Administrator: Command Prompt
C:\Windows\System32>tracert -d ww.yahoo.com

Tracing route to src.g03.yahoodns.net [18.136.37.69]
over a maximum of 30 hops:

  1  1 ms  <1 ms  <1 ms  192.168.50.1
  2  3 ms  2 ms  1 ms  192.168.100.1
  3  4 ms  3 ms  4 ms  203.210.148.86
  4  5 ms  5 ms  5 ms  123.25.17.73
  5  9 ms  4 ms  4 ms  113.171.32.25
  6  53 ms  53 ms  53 ms  113.171.34.42
  7  76 ms  70 ms  70 ms  113.171.27.90
  8  54 ms  53 ms  53 ms  113.171.50.222
  9  56 ms  56 ms  62 ms  113.171.36.53
 10  62 ms  61 ms  61 ms  99.83.116.138
 11  60 ms  58 ms  58 ms  52.93.11.142
 12  56 ms  58 ms  59 ms  52.93.11.63
 13  73 ms  78 ms  62 ms  52.93.11.60
 14  66 ms  70 ms  70 ms  52.93.8.161
 15  60 ms  58 ms  65 ms  203.83.223.31
 16  *      *      *      Request timed out.
 17  *      *      *      Request timed out.
 18  *      *      *      Request timed out.
 19  *      *      *      Request timed out.
 20  *      *      *      Request timed out.
 21  *      *      *      Request timed out.
 22  *      *      *      Request timed out.
 23  *      *      *      Request timed out.
 24  *      *      *      Request timed out.
```

Tương tự với câu lệnh “tracert -d www.yahoo.com” giúp em xem được đường truyền mạng từ máy tính của bạn tới máy chủ của trang web Yahoo đi qua những điểm nào và thời gian mất để đến được mỗi điểm đó. Tuy nhiên, do việc sử dụng “-d” trong câu lệnh, kết quả sẽ không hiển thị tên miền của các điểm dừng, mà chỉ hiển thị địa chỉ IP của chúng.

#### 4. Nslookup

```
Administrator: Command Prompt - nslookup
C:\Windows\System32>nslookup
Default Server:  RT-AX55-0618
Address:  192.168.50.1

> uniap.fpt.edu.vn
Server:  RT-AX55-0618
Address:  192.168.50.1

*** No internal type for both IPv4 and IPv6 Addresses (A+AAAA) records available for uniap.fpt.edu.vn
> set type=ns
> google.com
Server:  RT-AX55-0618
Address:  192.168.50.1

Non-authoritative answer:
google.com      nameserver = ns2.google.com
google.com      nameserver = ns4.google.com
google.com      nameserver = ns3.google.com
google.com      nameserver = ns1.google.com

ns2.google.com  internet address = 216.239.34.10
ns2.google.com  AAAA IPv6 address = 2001:4860:4802:34::a
ns4.google.com  internet address = 216.239.38.10
ns4.google.com  AAAA IPv6 address = 2001:4860:4802:38::a
ns3.google.com  internet address = 216.239.36.10
ns3.google.com  AAAA IPv6 address = 2001:4860:4802:36::a
ns1.google.com  internet address = 216.239.32.10
ns1.google.com  AAAA IPv6 address = 2001:4860:4802:32::a
>
```

Kết quả của câu lệnh này sẽ hiển thị danh sách các máy chủ tên (name servers) do có “set type=ns” được cấu hình cho tên miền "google.com". Các máy chủ tên này chịu trách nhiệm quản lý và cung cấp thông tin DNS cho tên miền đó. Kết quả bao gồm tên miền và địa chỉ IP của các máy chủ tên.

```
am C:\Users\adm>nslookup
n b Default Server:  RT-AX55-0618
    Address:  192.168.50.1

n > set type=mx
n > gmail.com
    Server:  RT-AX55-0618
    Address:  192.168.50.1

Non-authoritative answer:
ark gmail.com      MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
itcl gmail.com      MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
    gmail.com      MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com
    gmail.com      MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com
    gmail.com      MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com
m t > |
```

Kết quả của câu lệnh này sẽ hiển thị danh sách các máy chủ thư (mail servers) được cấu hình cho tên miền "gmail.com". Các máy chủ thư này chịu trách nhiệm nhận và xử lý email gửi tới tên miền đó. Kết quả thường bao gồm mức độ ưu tiên (priority) của máy chủ thư và địa chỉ IP hoặc tên miền của chúng.

## 5. Ipconfig

```
Administrator: Command Prompt

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

C:\Windows\System32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : LAPTOP-3GJTBRSD
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Unknown adapter VPN - VPN Client:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : VPN Client Adapter - VPN
Physical Address. . . . . : 5E-5C-02-E1-BD-5B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Unknown adapter OpenVPN Wintun:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Wintun Userspace Tunnel
Physical Address. . . . . :
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Unknown adapter Local Area Connection 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : TAP-Windows Adapter V9
Physical Address. . . . . : 00-FF-23-C9-D3-7F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Physical Address. . . . . : 04-ED-33-CF-A1-30
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Kết quả của câu lệnh “ipconfig /all” sẽ hiển thị thông tin về tất cả các giao diện mạng trên máy tính, bao gồm địa chỉ IP, địa chỉ MAC (Media Access Control), cấu hình DHCP (Dynamic Host Configuration Protocol), các địa chỉ DNS và các thông số mạng khác.

```
Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::afdd:e0bf:a802:97e0%15
    IPv4 Address. . . . . : 192.168.163.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

```
Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::98d6:6e02:d969:fb6c%8
    IPv4 Address. . . . . : 192.168.211.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

```
Ethernet adapter ZeroTier One [db64858fed92d0c9]:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::964d:8092:f753:bc29%22
    IPv4 Address. . . . . : 172.23.76.36
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 25.255.255.254
```

```
Ethernet adapter ZeroTier One [db64858fed241f01]:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::584d:811e:766e:3c8a%21
    IPv4 Address. . . . . : 10.243.76.36
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 25.255.255.254
```

```
Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1c67:6a02:1bcd:d436%13
    Default Gateway . . . . . :
```

```
Ethernet adapter Bluetooth Network Connection:

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

```
C:\Windows\System32>ipconfig /renew
```

**ipconfig /release** được sử dụng để giải phóng địa chỉ IP của một thiết bị từ mạng. Khi chạy lệnh này, thiết bị sẽ gửi một gói tin đặc biệt tới máy chủ DHCP (Dynamic Host Configuration Protocol) để yêu cầu giải phóng địa chỉ IP hiện tại. Ngược lại "**ipconfig /renew**" được sử dụng để yêu cầu máy tính nhận lại địa chỉ IP từ máy chủ DHCP

```

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::afdd:e0bf:a802:97e0%15
    IPv4 Address. . . . . : 192.168.163.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::98d6:6e02:d969:fb6c%8
    IPv4 Address. . . . . : 192.168.211.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter ZeroTier One [db64858fed92d0c9]:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::964d:8092:f753:bc29%22
    IPv4 Address. . . . . : 172.23.76.36
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 25.255.255.254

Ethernet adapter ZeroTier One [db64858fed241f01]:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::584d:811e:766e:3c8a%21
    IPv4 Address. . . . . : 10.243.76.36
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 25.255.255.254

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1c67:6a02:1bcd:d436%13
    IPv4 Address. . . . . : 192.168.50.85
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.50.1

Ethernet adapter Bluetooth Network Connection:

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

```

Tương tự câu lệnh “**ipconfig /release**” thì câu lệnh **ipconfig /renew** được sử dụng để yêu cầu cấp lại (renew) địa chỉ IP cho các giao diện mạng trên máy tính thông qua giao diện dòng lệnh trên hệ điều hành Windows.

```
C:\Windows\System32>ipconfig /displaydns
```

```
Windows IP Configuration
```

```
crl3.digicert.com
```

```
-----  
Record Name . . . . . : crl3.digicert.com  
Record Type . . . . . : 5  
Time To Live . . . . . : 2465  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : crl.edge.digicert.com
```

```
Record Name . . . . . : crl.edge.digicert.com  
Record Type . . . . . : 5  
Time To Live . . . . . : 2465  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : fp2e7a.wpc.2be4.phicdn.net
```

```
Record Name . . . . . : fp2e7a.wpc.2be4.phicdn.net  
Record Type . . . . . : 5  
Time To Live . . . . . : 2465  
Data Length . . . . . : 8  
Section . . . . . : Answer  
CNAME Record . . . . . : fp2e7a.wpc.phicdn.net
```

```
Record Name . . . . . : fp2e7a.wpc.phicdn.net  
Record Type . . . . . : 1  
Time To Live . . . . . : 2465  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 152.195.38.76
```

```
edgedl.me.gvt1.com
```

```
-----  
Record Name . . . . . : edgedl.me.gvt1.com  
Record Type . . . . . : 1  
Time To Live . . . . . : 47  
Data Length . . . . . : 4  
Section . . . . . : Answer  
A (Host) Record . . . . : 34.104.35.123
```

```
kubernetes.docker.internal
```

```
-----  
No records of type AAAA
```

```
kubernetes.docker.internal
```

```
-----  
Record Name . . . . . : kubernetes.docker.internal  
Record Type . . . . . : 1  
Time To Live . . . . . : 186875  
Data Length . . . . . : 4
```



**ipconfig /displaydns** nó sẽ hiển thị danh sách các bản ghi DNS đã được lưu trữ trong bộ nhớ cache của máy tính. Bộ nhớ cache DNS là nơi máy tính lưu trữ các thông tin DNS đã truy cập gần đây, bao gồm các địa chỉ IP tương ứng với tên miền đã truy vấn. Kết quả của câu lệnh này sẽ liệt kê các mục trong bộ nhớ cache DNS, bao gồm tên miền (Domain Name), loại bản ghi (Record Type), thời gian sống (Time to Live - TTL) và địa chỉ IP tương ứng (Data).

```
Record Name . . . . . : www.tm.ak.prd.aadg.trafficmanager.net
Record Type . . . . . : 1
Time To Live . . . . . : 210
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.190.144.162
```

```
C:\Windows\System32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\System32>_
```

**ipconfig /flushdns** nó sẽ xóa tất cả các bản ghi DNS đã được lưu trữ trong bộ nhớ cache của máy tính. Kết quả của câu lệnh này sẽ được thông báo một cách đơn giản trên màn hình.

```
C:\Windows\System32>ipconfig /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated.
Any errors will be reported in the Event Viewer in 15 minutes.

C:\Windows\System32>_
```

**ipconfig /registerdns** máy tính sẽ gửi yêu cầu đăng ký lại các bản ghi DNS của nó với máy chủ DNS trong mạng. Kết quả của câu lệnh này sẽ được thông báo một cách đơn giản trên màn hình.

## 6. Arp

```
C:\Windows\System32>arp -a

Interface: 192.168.211.1 --- 0x8
    Internet Address      Physical Address          Type
    192.168.211.255       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-fb        static
    224.0.0.252           01-00-5e-00-00-fc        static
    239.255.255.250       01-00-5e-7f-ff-fa        static

Interface: 192.168.50.85 --- 0xd
    Internet Address      Physical Address          Type
    192.168.50.1          04-42-1a-ba-06-18        dynamic
    192.168.50.222        80-47-86-ce-5a-58        dynamic
    192.168.50.255       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-fb        static
    224.0.0.252           01-00-5e-00-00-fc        static
    239.255.255.250       01-00-5e-7f-ff-fa        static
    255.255.255.255       ff-ff-ff-ff-ff-ff        static

Interface: 192.168.163.1 --- 0xf
    Internet Address      Physical Address          Type
    192.168.163.255       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-fb        static
    224.0.0.252           01-00-5e-00-00-fc        static
    239.255.255.250       01-00-5e-7f-ff-fa        static

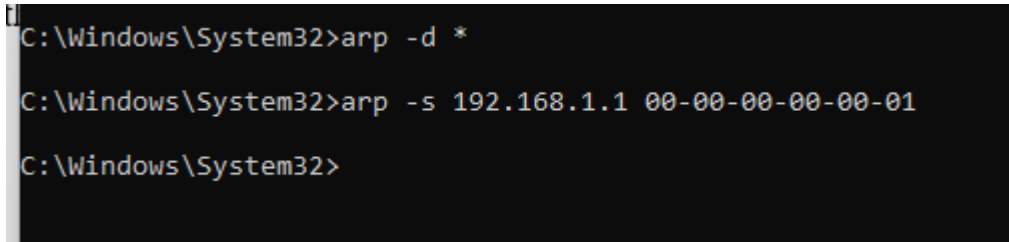
Interface: 10.243.76.36 --- 0x15
    Internet Address      Physical Address          Type
    10.243.255.255        ff-ff-ff-ff-ff-ff        static
    25.255.255.254        12-00-bc-ae-17-68        static
    224.0.0.22            01-00-5e-00-00-16        static
    224.0.0.251           01-00-5e-00-00-fb        static
    224.0.0.252           01-00-5e-00-00-fc        static
    239.255.255.250       01-00-5e-7f-ff-fa        static

Interface: 172.23.76.36 --- 0x16
    Internet Address      Physical Address          Type
    25.255.255.254        da-00-bf-61-36-d6        static
    172.23.255.255        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-fb        static
    224.0.0.252           01-00-5e-00-00-fc        static
    239.255.255.250       01-00-5e-7f-ff-fa        static

C:\Windows\System32>
```

**arp -a** nó sẽ hiển thị danh sách các địa chỉ IP và địa chỉ MAC (Media Access Control) tương ứng trong bảng ARP của máy tính. Bảng ARP là một bảng chứa thông tin về các liên kết giữa địa chỉ IP và địa chỉ MAC trong mạng. Kết quả

của câu lệnh này sẽ hiển thị danh sách các mục trong bảng ARP, bao gồm địa chỉ IP (Internet Protocol), địa chỉ MAC, loại giao thức và giao diện mạng tương ứng.



```
C:\Windows\System32>arp -d *  
  
C:\Windows\System32>arp -s 192.168.1.1 00-00-00-00-00-01  
  
C:\Windows\System32>
```

**arp -d \*** nó sẽ xóa tất cả các mục trong bảng ARP của máy tính. Kết quả của câu lệnh này sẽ không được hiển thị trên màn hình.

Khi thực hiện câu lệnh **arp -s 192.168.1.1 00-00-00-00-00-01** nó sẽ thêm (set) một mục mới vào bảng ARP của máy tính với địa chỉ IP "192.168.1.1" và địa chỉ MAC "00-00-00-00-00-01". Điều này sẽ tạo ra một liên kết giữa địa chỉ IP và địa chỉ MAC trong mạng.

## 7. Netstat

**netstat** mà không có tùy chọn bổ sung hoặc tùy chọn default “-f”, nó sẽ hiển thị danh sách các kết nối mạng hiện tại trên máy tính. Thông tin được hiển thị bao gồm các kết nối TCP (Transmission Control Protocol) và UDP (User Datagram Protocol), cả trong và ngoài mạng. Kết quả của câu lệnh này sẽ liệt kê các kết nối mạng hiện tại, bao gồm địa chỉ IP và cổng của máy tính local, địa chỉ IP và cổng của máy tính remote, trạng thái kết nối (như ESTABLISHED, LISTENING, WAITING, và CLOSED), và giao thức (TCP hoặc UDP) của mỗi kết nối.

```
C:\Windows\System32>netstat -f

Active Connections

Proto Local Address           Foreign Address         State
TCP    127.0.0.1:9930          kubernet.es:32240      ESTABLISHED
TCP    127.0.0.1:9930          kubernet.es:32242      ESTABLISHED
TCP    127.0.0.1:32240        kubernet.es:9930       ESTABLISHED
TCP    127.0.0.1:32242        kubernet.es:9930       ESTABLISHED
TCP    127.0.0.1:49673        kubernet.es:49674      ESTABLISHED
TCP    127.0.0.1:49674        kubernet.es:49673      ESTABLISHED
TCP    192.168.50.85:32687    20.198.119.84:https    ESTABLISHED
TCP    192.168.50.85:32706    tg-in-f188.1e100.net:5228 ESTABLISHED
TCP    192.168.50.85:32707    tg-in-f188.1e100.net:5228 ESTABLISHED
TCP    192.168.50.85:32720    edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP    192.168.50.85:32722    edge-dgw-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP    192.168.50.85:32723    edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP    192.168.50.85:32724    edge-z-p3-shv-01-hkt1.facebook.com:https ESTABLISHED
TCP    192.168.50.85:32726    edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP    192.168.50.85:32728    h1-epnsbroker04.eset.com:8883 ESTABLISHED
TCP    192.168.50.85:32749    52.139.250.209:https    ESTABLISHED
TCP    192.168.50.85:32753    52.139.250.209:https    ESTABLISHED
TCP    192.168.50.85:32937    hkg07s41-in-f14.1e100.net:https ESTABLISHED
TCP    192.168.50.85:32939    kul09s03-in-f3.1e100.net:https ESTABLISHED
TCP    192.168.50.85:32963    ec2-54-71-149-230.us-west-2.compute.amazonaws.com:https TIME_WAIT
TCP    192.168.50.85:32966    ec2-34-213-94-47.us-west-2.compute.amazonaws.com:https TIME_WAIT
TCP    [fe80::584d:811e:766e:3c8a%21]:8391 LAPTOP-3GJTBRSD:32245 ESTABLISHED
TCP    [fe80::584d:811e:766e:3c8a%21]:32245 LAPTOP-3GJTBRSD:8391 ESTABLISHED

C:\Windows\System32>
```

**netstat -o** nó sẽ hiển thị danh sách các kết nối mạng hiện tại cùng với mã số quy trình (PID - Process Identifier) của quy trình liên quan đến mỗi kết nối. Thông tin này giúp xác định quy trình nào đang tạo ra hoặc sử dụng kết nối mạng. Kết quả của câu lệnh này sẽ liệt kê các kết nối mạng hiện tại cùng với địa chỉ IP và cổng của máy tính local, địa chỉ IP và cổng của máy tính remote, trạng thái kết nối và mã số quy trình của quy trình liên quan.

```
C:\Windows\System32>netstat -o

Active Connections

Proto Local Address           Foreign Address         State      PID
TCP    127.0.0.1:9930          kubernet.es:32240      ESTABLISHED 6404
TCP    127.0.0.1:9930          kubernet.es:32242      ESTABLISHED 6404
TCP    127.0.0.1:32240        kubernet.es:9930       ESTABLISHED 16404
TCP    127.0.0.1:32242        kubernet.es:9930       ESTABLISHED 16404
TCP    127.0.0.1:49673        kubernet.es:49674      ESTABLISHED 7320
TCP    127.0.0.1:49674        kubernet.es:49673      ESTABLISHED 7320
TCP    192.168.50.85:32687    20.198.119.84:https    ESTABLISHED 6992
TCP    192.168.50.85:32706    tg-in-f188.1e100.net:5228 ESTABLISHED 2272
TCP    192.168.50.85:32707    tg-in-f188.1e100.net:5228 ESTABLISHED 2272
TCP    192.168.50.85:32720    edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED 2272
TCP    192.168.50.85:32722    edge-dgw-shv-02-hkt1.facebook.com:https ESTABLISHED 2272
TCP    192.168.50.85:32723    edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED 2272
TCP    192.168.50.85:32724    edge-z-p3-shv-01-hkt1.facebook.com:https ESTABLISHED 2272
TCP    192.168.50.85:32726    edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED 2272
TCP    192.168.50.85:32728    h1-epnsbroker04.eset.com:8883 ESTABLISHED 2848
TCP    192.168.50.85:32749    52.139.250.209:https    ESTABLISHED 2272
TCP    192.168.50.85:32753    52.139.250.209:https    ESTABLISHED 2272
TCP    192.168.50.85:32937    sin10s06-in-f10.1e100.net:https ESTABLISHED 2272
TCP    192.168.50.85:32975    kul06s17-in-f238.1e100.net:https ESTABLISHED 2272
TCP    192.168.50.85:32979    ec2-54-71-149-230.us-west-2.compute.amazonaws.com:https TIME_WAIT 0
TCP    192.168.50.85:32980    ec2-34-213-94-47.us-west-2.compute.amazonaws.com:https TIME_WAIT 0
TCP    192.168.50.85:32984    90:https               TIME_WAIT 0
TCP    [fe80::584d:811e:766e:3c8a%21]:8391 LAPTOP-3GJTBRSD:32245 ESTABLISHED 4
TCP    [fe80::584d:811e:766e:3c8a%21]:32245 LAPTOP-3GJTBRSD:8391 ESTABLISHED 18168

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

**netstat -n** nó sẽ hiển thị danh sách các kết nối mạng hiện tại mà không giải quyết (resolve) địa chỉ IP thành tên miền. Thay vào đó, địa chỉ IP được hiển thị dưới dạng địa chỉ IP thuần túy. Kết quả của câu lệnh này sẽ liệt kê các kết nối mạng hiện tại, bao gồm địa chỉ IP và cổng của máy tính local, địa chỉ IP và cổng của máy tính remote, trạng thái kết nối và giao thức (TCP hoặc UDP) của mỗi kết nối.

```
C:\Windows\System32>netstat -n

Active Connections

Proto Local Address          Foreign Address         State
TCP    127.0.0.1:9930          127.0.0.1:32240        ESTABLISHED
TCP    127.0.0.1:9930          127.0.0.1:32242        ESTABLISHED
TCP    127.0.0.1:32240        127.0.0.1:9930         ESTABLISHED
TCP    127.0.0.1:32242        127.0.0.1:9930         ESTABLISHED
TCP    127.0.0.1:49673        127.0.0.1:49674        ESTABLISHED
TCP    127.0.0.1:49674        127.0.0.1:49673        ESTABLISHED
TCP    192.168.50.85:32687    20.198.119.84:443       ESTABLISHED
TCP    192.168.50.85:32706    74.125.23.188:5228      ESTABLISHED
TCP    192.168.50.85:32707    74.125.23.188:5228      ESTABLISHED
TCP    192.168.50.85:32720    31.13.75.1:443          ESTABLISHED
TCP    192.168.50.85:32722    31.13.75.10:443         ESTABLISHED
TCP    192.168.50.85:32723    31.13.75.1:443          ESTABLISHED
TCP    192.168.50.85:32724    31.13.77.54:443         ESTABLISHED
TCP    192.168.50.85:32726    31.13.75.1:443          ESTABLISHED
TCP    192.168.50.85:32728    91.228.165.147:8883     ESTABLISHED
TCP    192.168.50.85:32749    52.139.250.209:443      ESTABLISHED
TCP    192.168.50.85:32753    52.139.250.209:443      ESTABLISHED
TCP    192.168.50.85:32973    172.217.24.74:443       ESTABLISHED
TCP    192.168.50.85:32975    172.217.24.238:443      ESTABLISHED
TCP    192.168.50.85:32985    20.189.173.12:443       ESTABLISHED
TCP    192.168.50.85:32987    40.126.35.87:443        ESTABLISHED
TCP    192.168.50.85:32992    204.79.197.203:443      ESTABLISHED
TCP    192.168.50.85:32993    54.71.149.230:443       TIME_WAIT
TCP    192.168.50.85:32994    34.210.161.87:443       TIME_WAIT
TCP    192.168.50.85:32995    10.33.75.158:7680       SYN_SENT
TCP    192.168.50.85:32996    10.33.18.160:7680       SYN_SENT
TCP    [fe80::584d:811e:766e:3c8a%21]:8391 [fe80::584d:811e:766e:3c8a%21]:32245 ESTABLISHED
TCP    [fe80::584d:811e:766e:3c8a%21]:32245 [fe80::584d:811e:766e:3c8a%21]:8391 ESTABLISHED

C:\Windows\System32>
```

**netstat -a** nó sẽ hiển thị danh sách tất cả các kết nối mạng hiện tại và các cổng lắng nghe trên máy tính của bạn. Thông tin được hiển thị bao gồm cả kết nối TCP và UDP, cả trong và ngoài mạng. Kết quả của câu lệnh này sẽ liệt kê các kết nối mạng hiện tại cùng với địa chỉ IP và cổng của máy tính local, địa chỉ IP và cổng của máy tính remote, trạng thái kết nối và giao thức (TCP hoặc UDP) của mỗi kết nối. Ngoài ra, nó cũng sẽ hiển thị các cổng mà máy tính đang lắng nghe kết nối từ các máy khác.

```
C:\Windows\System32>netstat -a
```

#### Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:135	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:443	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:445	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:808	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:902	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:912	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:2382	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:3306	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:5040	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:6646	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:7680	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:8391	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:9930	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49664	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49665	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49666	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49667	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49668	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49670	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49671	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49682	LAPTOP-3GJTBRSD:0	LISTENING
TCP	0.0.0.0:49919	LAPTOP-3GJTBRSD:0	LISTENING
TCP	10.243.76.36:139	LAPTOP-3GJTBRSD:0	LISTENING
TCP	127.0.0.1:5939	LAPTOP-3GJTBRSD:0	LISTENING
TCP	127.0.0.1:9930	kubernetes:32240	ESTABLISHED
TCP	127.0.0.1:9930	kubernetes:32242	ESTABLISHED
TCP	127.0.0.1:9983	LAPTOP-3GJTBRSD:0	LISTENING
TCP	127.0.0.1:9993	LAPTOP-3GJTBRSD:0	LISTENING
TCP	127.0.0.1:32240	kubernetes:9930	ESTABLISHED
TCP	127.0.0.1:32242	kubernetes:9930	ESTABLISHED
TCP	127.0.0.1:47582	LAPTOP-3GJTBRSD:0	LISTENING
TCP	127.0.0.1:49673	kubernetes:49674	ESTABLISHED
TCP	127.0.0.1:49674	kubernetes:49673	ESTABLISHED
TCP	127.0.0.1:64492	LAPTOP-3GJTBRSD:0	LISTENING
TCP	172.23.76.36:139	LAPTOP-3GJTBRSD:0	LISTENING
TCP	192.168.50.85:139	LAPTOP-3GJTBRSD:0	LISTENING
TCP	192.168.50.85:9993	LAPTOP-3GJTBRSD:0	LISTENING
TCP	192.168.50.85:32687	20.198.119.84:https	ESTABLISHED
TCP	192.168.50.85:32706	tg-in-f188:5228	ESTABLISHED
TCP	192.168.50.85:32707	tg-in-f188:5228	ESTABLISHED
TCP	192.168.50.85:32720	edge-star-shv-02-hkt1:https	ESTABLISHED
TCP	192.168.50.85:32722	edge-dgw-shv-02-hkt1:https	ESTABLISHED
TCP	192.168.50.85:32723	edge-star-shv-02-hkt1:https	ESTABLISHED
TCP	192.168.50.85:32724	edge-z-p3-shv-01-hkt1:https	ESTABLISHED
TCP	192.168.50.85:32726	edge-star-shv-02-hkt1:https	ESTABLISHED
TCP	192.168.50.85:32728	h1-epnsbroker04:8883	ESTABLISHED
TCP	192.168.50.85:32749	52.139.250.209:https	ESTABLISHED
TCP	192.168.50.85:32753	52.139.250.209:https	ESTABLISHED
TCP	192.168.50.85:32973	sin10s06-in-f10:https	ESTABLISHED
TCP	192.168.50.85:32975	kul06s17-in-f238:https	ESTABLISHED
TCP	192.168.50.85:32985	20.189.173.12:https	ESTABLISHED
TCP	192.168.50.85:32987	40.126.35.87:https	ESTABLISHED
TCP	192.168.50.85:32992	a-0003:https	ESTABLISHED
TCP	192.168.50.85:32997	10.33.11.22:ms-do	SYN_SENT
TCP	192.168.50.85:32998	10.33.72.196:ms-do	SYN_SENT

**netstat -s -p tcp -f** nó sẽ hiển thị các thống kê về các kết nối TCP, bao gồm số lượng kết nối thành công, số lượng kết nối thất bại, số lượng gói tin đã được gửi và nhận, cũng như các thống kê khác liên quan đến TCP. Kết quả của câu lệnh này sẽ hiển thị thông tin thống kê chi tiết về các kết nối TCP trên máy tính.



```
C:\Windows\System32>netstat -s -p tcp -f

TCP Statistics for IPv4

Active Opens           = 27577
Passive Opens          = 207
Failed Connection Attempts = 3508
Reset Connections      = 3143
Current Connections    = 19
Segments Received      = 1418229
Segments Sent          = 1002069
Segments Retransmitted  = 14005

Active Connections

Proto Local Address           Foreign Address         State
TCP   127.0.0.1:9930           kubernet.es.docker.internal:32240 ESTABLISHED
TCP   127.0.0.1:9930           kubernet.es.docker.internal:32242 ESTABLISHED
TCP   127.0.0.1:32240         kubernet.es.docker.internal:9930 ESTABLISHED
TCP   127.0.0.1:32242         kubernet.es.docker.internal:9930 ESTABLISHED
TCP   127.0.0.1:49673         kubernet.es.docker.internal:49674 ESTABLISHED
TCP   127.0.0.1:49674         kubernet.es.docker.internal:49673 ESTABLISHED
TCP   192.168.50.85:32687     20.198.119.84:https      ESTABLISHED
TCP   192.168.50.85:32706     tg-in-f188.1e100.net:5228 ESTABLISHED
TCP   192.168.50.85:32707     tg-in-f188.1e100.net:5228 ESTABLISHED
TCP   192.168.50.85:32720     edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP   192.168.50.85:32722     edge-dgw-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP   192.168.50.85:32723     edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP   192.168.50.85:32724     edge-z-p3-shv-01-hkt1.facebook.com:https ESTABLISHED
TCP   192.168.50.85:32726     edge-star-shv-02-hkt1.facebook.com:https ESTABLISHED
TCP   192.168.50.85:32728     h1-epnsbroker04.eset.com:8883 ESTABLISHED
TCP   192.168.50.85:32749     52.139.250.209:https      ESTABLISHED
TCP   192.168.50.85:32753     52.139.250.209:https      ESTABLISHED
TCP   192.168.50.85:33014     51.104.167.245:https      ESTABLISHED
TCP   192.168.50.85:33016     ec2-54-71-149-230.us-west-2.compute.amazonaws.com:https TIME_WAIT
TCP   192.168.50.85:33017     ec2-34-210-161-87.us-west-2.compute.amazonaws.com:https TIME_WAIT
TCP   192.168.50.85:33018     20.189.173.12:https       ESTABLISHED
```

**netstat -e** được sử dụng để hiển thị thông kê về lưu lượng mạng trên hệ điều hành Windows. Nó sẽ hiển thị các thông tin như số lượng gói tin đã được gửi và nhận, lỗi truyền thông, lưu lượng mạng và các thông số khác liên quan đến giao thức mạng. Với “-t 5” các kết quả mới sẽ được trả về mỗi 5s.

```
C:\Windows\System32>netstat -e -t 5
Interface Statistics
```

	Received	Sent
Bytes	2828726474	251232472
Unicast packets	2633610	1019493
Non-unicast packets	39095	23121
Discards	0	0
Errors	0	0
Unknown protocols	0	

Interface Statistics

	Received	Sent
Bytes	2828726474	251232472
Unicast packets	2633610	1019493
Non-unicast packets	39095	23121
Discards	0	0
Errors	0	0
Unknown protocols	0	

Interface Statistics

	Received	Sent
Bytes	2828926520	251460371
Unicast packets	2634212	1020081
Non-unicast packets	39123	23135
Discards	0	0
Errors	0	0
Unknown protocols	0	

Interface Statistics

	Received	Sent
Bytes	2828926520	251460371
Unicast packets	2634212	1020081
Non-unicast packets	39123	23135
Discards	0	0
Errors	0	0
Unknown protocols	0	

Interface Statistics

	Received	Sent
Bytes	2829148707	252233213
Unicast packets	2635612	1021705
Non-unicast packets	39151	23483
Discards	0	0
Errors	0	0
Unknown protocols	0	

Interface Statistics

	Received	Sent
Bytes	2829148707	252233213
Unicast packets	2635612	1021705



