Hướng dẫn dùng lệnh netstat để quản lý mạng trên CentOS

Netstat (network statistics) là một công cụ dòng lệnh để theo dõi các kết nối mạng vào và ra có sẵn trên tất cả các hệ điều hành dựa trên Unix và cũng có sẵn trên hệ điều hành Windows. Nó rất hữu ích trong việc khắc phục sự cố mạng và đo lường hiệu năng. **Netstat** là một trong những công cụ gỡ lỗi dịch vụ mạng cơ bản nhất, cho bạn biết cổng nào mở và bất kỳ chương trình nào đang lắng nghe trên các cổng.

Trong bài này Kỹ thuật sẽ hướng dẫn các bạn sử dụng lệnh **netstat** để quản lý mạng trên CentOS 6 64bit bằng một số ví dụ trực quan.

Liệt kê tất cả các cổng của các kết nối TCP và UDP

```
# netstat -a | more
```

```
[root@mail hello]# netstat -a | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 mail.quanglan.name.vn:ssh   182.100.67.40:47920         ESTABLISHED
tcp        0     64 mail.quanglan.name.vn:ssh   vpn01.infra.123host.v:51784 ESTABLISHED
tcp        0      0 *:ssh                       *:*                         LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     9317   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     6970   @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     9550   @/var/run/hald/dbus-T1upiWias8
unix  2      [ ]         DGRAM                    9634   @/org/freedesktop/hal/udev_event
unix  2      [ ]         DGRAM                    7402   @/org/kernel/udev/udevd
unix  2      [ ACC ]     STREAM     LISTENING     9555   @/var/run/hald/dbus-xgqmYpEwjG
unix  2      [ ACC ]     STREAM     LISTENING     5845   @/ply-boot-protocol
unix  5      [ ]         DGRAM                    8520945 /dev/log
unix  2      [ ]         DGRAM                    8552408
unix  3      [ ]         STREAM     CONNECTED     8552401
unix  3      [ ]         STREAM     CONNECTED     8552400
unix  2      [ ]         DGRAM                    8540100
unix  2      [ ]         DGRAM                    8524315
unix  2      [ ]         DGRAM                    8470164
unix  2      [ ]         DGRAM                    723947
unix  3      [ ]         STREAM     CONNECTED     11948  /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     11947
```

Liệt kê tất cả các cổng kết nối TCP

```
# netstat -at
```

```
[root@mail hello]# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0     64 mail.quanglan.name.vn:ssh   -                           ESTABLISHED
tcp        0      0 mail.quanglan.name.vn:ssh   182.100.67.40:61885         ESTABLISHED
tcp        0      0 *:ssh                       *:*                         LISTEN
```

Liệt kê tất cả các cổng kết nối UDP

```
# netstat -au
```

```
[root@lantq02 ~]# netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 lantq02.123host.vn:domain   *:*
udp        0      0 localhost.localdomain:domain *:*
```

Liệt kê tất cả các kết nối đang lắng nghe

```
# netstat -l
```

```
[root@mail hello]# netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     9317   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     6970   @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     9550   @/var/run/hald/dbus-T1upiWias8
unix  2      [ ACC ]     STREAM     LISTENING     9555   @/var/run/hald/dbus-xgqmYpEwjG
unix  2      [ ACC ]     STREAM     LISTENING     5845   @/ply-boot-protocol
```

Liệt kê tất cả các cổng TCP đang lắng nghe

```
# netstat -lt
```

```
[root@mail hello]# netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
```

Liệt kê tất cả các cổng UCP đang lắng nghe

```
# netstat -lu
```

```
[root@lantq02 ~]# netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 lantq02.123host.vn:domain   *:*
udp        0      0 localhost.localdomain:domain *:*
```

Liệt kê tất cả các cổng Unix đang lắng nghe

```
# netstat -lx
```

```
[root@mail hello]# netstat -lx
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node Path
unix  2      [ ACC ]     STREAM     LISTENING     9317   /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     STREAM     LISTENING     6970   @/com/ubuntu/upstart
unix  2      [ ACC ]     STREAM     LISTENING     9550   @/var/run/hald/dbus-T1upiWias8
unix  2      [ ACC ]     STREAM     LISTENING     9555   @/var/run/hald/dbus-xgqmYpEwjG
unix  2      [ ACC ]     STREAM     LISTENING     5845   @/ply-boot-protocol
```

Hiển thị thống kê qua từng giao thức

```
# netstat -s
```

```
[root@mail hello]# netstat -s
Ip:
    1751669 total packets received
    6954 with invalid addresses
    0 forwarded
    0 incoming packets discarded
    1744715 incoming packets delivered
    1491804 requests sent out
Icmp:
    14750 ICMP messages received
    14 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 14356
        timeout in transit: 1
        echo requests: 389
        echo replies: 4
    16626 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 16237
        echo replies: 389
IcmpMsg:
        InType0: 4
        InType3: 14356
        InType8: 389
        InType11: 1
        OutType0: 389
        OutType3: 16237
Tcp:
    10130 active connections openings
    19247 passive connection openings
    2830 failed connection attempts
    6228 connection resets received
    2 connections established
    1579642 segments received
    1414941 segments send out
    8276 segments retransmited
    10 bad segments received.
    36775 resets sent
Udp:
    38202 packets received
    16286 packets to unknown port received.
    0 packet receive errors
    53847 packets sent
```

Hiển thị thống kê theo giao thức TCP

```
# netstat -st
```

```
[root@mail hello]# netstat -st
IcmpMsg:
    InType0: 4
    InType3: 14356
    InType8: 389
    InType11: 1
    OutType0: 389
    OutType3: 16237
Tcp:
    10130 active connections openings
    19257 passive connection openings
    2830 failed connection attempts
    6228 connection resets received
    2 connections established
    1579935 segments received
    1415226 segments send out
    8281 segments retransmited
    10 bad segments received.
    36797 resets sent
UdpLite:
TcpExt:
    9416 invalid SYN cookies received
    424 resets received for embryonic SYN_RECV sockets
    3 packets pruned from receive queue because of socket buffer overrun
    1712 TCP sockets finished time wait in fast timer
    44856 delayed acks sent
    38 delayed acks further delayed because of locked socket
    Quick ack mode was activated 5295 times
    167935 packets directly queued to recvmsg prequeue.
    674558 packets directly received from backlog
    275600483 packets directly received from prequeue
    732280 packets header predicted
    137896 packets header predicted and directly queued to user
    105524 acknowledgments not containing data received
    402931 predicted acknowledgments
    TCPDSACKUndo: 7
    506 congestion windows recovered after partial ack
    0 TCP data loss events
    381 timeouts after SACK recovery
    11 timeouts in loss state
    73 retransmits in slow start
    5555 other TCP timeouts
    767 packets collapsed in receive queue due to low socket buffer
    5301 DSACKs sent for old packets
    471 DSACKs received
    6051 connections reset due to unexpected data
```


Hiển thị thống kê theo giao thức UDP

```
# netstat -su
```

```
[root@mail hello]# netstat -su
IcmpMsg:
    InType0: 4
    InType3: 14356
    InType8: 389
    InType11: 1
    OutType0: 389
    OutType3: 16237
Udp:
    38216 packets received
    16286 packets to unknown port received.
    0 packet receive errors
    53861 packets sent
UdpLite:
IpExt:
    InMcastPkts: 3212
    InBcastPkts: 94603
    InOctets: 4916136793
    OutOctets: 858650177
    InMcastOctets: 102784
    InBcastOctets: 53984894
```

Hiển thị tên dịch vụ với PID

netstat -tp

```
[root@mail hello]# netstat -tp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 mail.quanglan.name.vn:ssh   182.100.67.40:49720         ESTABLISHED
tcp        0     64 mail.quanglan.name.vn:ssh   vpn01.infra.123host.v:51784 ESTABLISHED
```

Hiển thị trong Promiscuous mode

Khi chạy lệnh này thì sau một khoảng thời gian chỉ định, **netstat** sẽ làm mới lại và in ra màn hình kết quả.

netstat -ac -5 | grep tcp

```
[root@mail hello]# netstat -ac 5 | grep tcp
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0     64 mail.quanglan.name.vn:ssh   vpn01.infra.123host.v:51784 ESTABLISHED
tcp        0      0 mail.quanglan.name.vn:ssh   182.100.67.40:36124         ESTABLISHED
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 *:ssh                       *:*                         LISTEN
tcp        0      0 mail.quanglan.name.vn:ssh   vpn01.infra.123host.v:51784 ESTABLISHED
tcp        0      0 mail.quanglan.name.vn:ssh   182.100.67.40:16733         ESTABLISHED
tcp        0      0 *:ssh                       *:*                         LISTEN
^C
[root@mail hello]#
```

Hiển thị bảng định tuyến

netstat -r

```
[root@mail hello]# netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
103.255.236.128 *               255.255.255.128 U         0 0          0 eth0
link-local      *               255.255.0.0     U         0 0          0 eth0
default         no-ptr.123host. 0.0.0.0         UG        0 0          0 eth0
```

Hiển thị trao đổi gói trên cổng mạng

Hiển thị các gói nhận và chuyển trên cổng mạng với đơn vị MTU

netstat -i

```
[root@mail hello]# netstat -i
Kernel Interface table
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0       1500   0 17745954      0      0      0   753700      0      0      0 BMRU
lo        65536   0   748081      0      0      0   748081      0      0      0 LRU
```

Hiển thị thông tin cổng mạng

Lệnh này tương tự lệnh **ifconfig**

netstat -ie

```
[root@mail hello]# netstat -ie
Kernel Interface table
eth0      Link encap:Ethernet  HWaddr 12:EA:3D:04:6D:9E
          inet addr:103.255.236.197  Bcast:103.255.236.255  Mask:255.255.255.128
          inet6 addr: fe80::10ea:3dff:fe04:6d9e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:17772314 errors:0 dropped:0 overruns:0 frame:0
          TX packets:754226 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5175631754 (4.8 GiB)  TX bytes:95533588 (91.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:748081 errors:0 dropped:0 overruns:0 frame:0
          TX packets:748081 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:774547917 (738.6 MiB)  TX bytes:774547917 (738.6 MiB)
```

Hiển thị thông tin IPv4, IPV6

netstat -g

```
[root@mail hello]# netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      all-systems.mcast.net
lo              1      ff02::1
eth0            1      ff02::1:ff04:6d9e
eth0            1      ff02::1
```

Hiển thị một chương trình nào đó đang chạy port nào

netstat -ap | grep <name of service>

```
[root@lantq02 ~]# netstat -ap | grep http
tcp        0      0 *:http                      *:*                         LISTEN      9589/httpd
tcp        0      0 *:https                     *:*                         LISTEN      9589/httpd
```

Từ những lệnh trên, ta có thể kiểm tra xem các dịch vụ nào đang chạy trên các port nào bằng cách dùng lệnh sau:

netstat -tulpn

Hoặc:

netstat -tulpn | grep <name of service>

```
[root@lantq02 ~]# netstat -tulpn | grep httpd
tcp        0      0 0.0.0.0:80                  0.0.0.0:*                   LISTEN      9589/httpd
tcp        0      0 0.0.0.0:443                 0.0.0.0:*                   LISTEN      9589/httpd
```

Trên đây là một số ví dụ sử dụng lệnh netstat để quản lý mạng trên CentOs 6.