



[hiva-network.com](http://hiva-network.com)

## آموزش کامل فرمان Netstat بخش دوم

مولف : گروه آموزشی هیوا شبکه

آدرس : رشت - خیابان بیستون - بن بست زارع - ساختمان پویا - طبقه دوم - واحد ۳

تلفن: ۰۱۳۳۳۲۴۱۲۶۹ - ۰۱۳۳۳۲۶۰۰۴۱

همراه : ۰۹۱۱۴۵۴۵۱۹۳

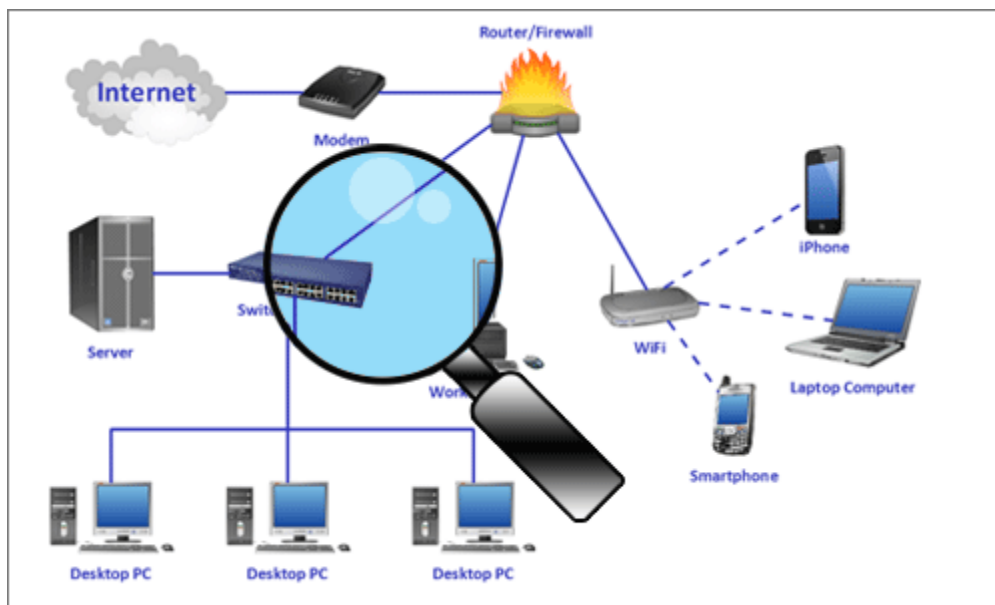
ارتباط با ما:

کانال تلگرام: @hivashabake

Students@hiva-network.com

<http://www.hiva-network.com>

## آموزش کامل فرمان Netstat بخش دوم



سلام به همه شما دوستان و همراهان همیشگی هیوا

در این آموزش بخش دوم فرمان NETSTAT و Switch های آن را بررسی کنیم.

Netstat -o

این سوئیچ Process ID یا PID مربوط به برنامه ای که Connection مربوط به آن است را نشان می دهد. این سوئیچ یک ستون دیگر با عنوان PID به خروجی های netstat می افزاید.

netstat -no<

```

Administrator: Windows PowerShell
PS C:\hiva> netstat -no

Active Connections

Proto Local Address           Foreign Address         State                   PID
----
TCP   127.0.0.1:15485         127.0.0.1:51937        ESTABLISHED            1832
TCP   127.0.0.1:50026         127.0.0.1:50027        ESTABLISHED            1164
TCP   127.0.0.1:50027         127.0.0.1:50026        ESTABLISHED            1164
TCP   127.0.0.1:51937         127.0.0.1:15485        ESTABLISHED            3744
PS C:\hiva>
  
```

Netstat -p

با این سوئیچ می توانید خروجی netstat را بر اساس یکی از پروتکل های زیر فیلتر کنید:

tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, ipv6

برای مثال

Netstat -a -p udpv6<

```

Administrator: Windows PowerShell
PS C:\hiva> netstat -ap udpv6

Active Connections

Proto Local Address           Foreign Address         State
UDP   [::]:123                *:*
UDP   [::]:500                *:*
UDP   [::]:3702               *:*
UDP   [::]:3702               *:*
UDP   [::]:3702               *:*
UDP   [::]:3702               *:*
UDP   [::]:3702               *:*
UDP   [::]:4500               *:*
UDP   [::]:5355               *:*
UDP   [::]:53245              *:*
UDP   [::]:53247              *:*
UDP   [::]:55914              *:*
UDP   [::]:58663              *:*
UDP   [::]:63019              *:*
UDP   [::]:63021              *:*
UDP   [::]:64734              *:*
UDP   [::1]:1900               *:*
UDP   [::1]:5353               *:*
UDP   [::1]:56019             *:*
UDP   [fe80::4512:8565:21cb:880a%16]:5353 *:*
UDP   [fe80::a52a:1267:4293:3b0b%4]:1900  *:*
UDP   [fe80::a52a:1267:4293:3b0b%4]:56018 *:*

PS C:\hiva>
  
```

Netstat -r

فرمان معادل فرمان `route print` است. IPv4 Routing Table و IPv6 Routing Table را می توانید با این فرمان ببینید. خروجی این

Netstat -r<

```

Administrator: Command Prompt

C:\Hiva>netstat -r

=====
Interface List
 5...1a ee 65 6f 20 c2 .....Microsoft Wi-Fi Direct Virtual Adapter
 4...b8 ee 65 6f 20 c2 .....Qualcomm Atheros AR956x Wireless Network Adapter
 1.....Software Loopback Interface 1
14...00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
15...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway           Interface         Metric
0.0.0.0                    0.0.0.0          192.168.1.1       192.168.1.4       25
127.0.0.0                  255.0.0.0        On-link           127.0.0.1         306
127.0.0.1                  255.255.255.255 On-link           127.0.0.1         306
127.255.255.255           255.255.255.255 On-link           127.0.0.1         306
192.168.1.0                255.255.255.0   On-link           192.168.1.4       281
192.168.1.4                255.255.255.255 On-link           192.168.1.4       281
192.168.1.255             255.255.255.255 On-link           192.168.1.4       281
224.0.0.0                  240.0.0.0        On-link           127.0.0.1         306
224.0.0.0                  240.0.0.0        On-link           192.168.1.4       281
255.255.255.255           255.255.255.255 On-link           127.0.0.1         306
255.255.255.255           255.255.255.255 On-link           192.168.1.4       281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
14    306  ::/0                On-link
1     306  ::1/128             On-link
14    306  2001::/32           On-link
14    306  2001:0:9d38:6ab8:10bc:21cf:3f57:fefb/128
On-link
4     281  fe80::/64           On-link
14    306  fe80::/64           On-link
14    306  fe80::10bc:21cf:3f57:fefb/128
On-link
4     281  fe80::a52a:1267:4293:3b0b/128
On-link
1     306  ff00::/8            On-link
4     281  ff00::/8            On-link
14    306  ff00::/8            On-link
=====
Persistent Routes:
None

C:\Hiva>
  
```

هیوا شبکه

Netstat -s

برای هر یک از پروتکل های گفته شده در netstat -p آمار کاملی را نشان می دهد.

## Netstat -s<

```

C:\Hiva>netstat -s

IPv4 Statistics

Packets Received                = 81498
Received Header Errors          = 0
Received Address Errors        = 0
Datagrams Forwarded            = 0
Unknown Protocols Received     = 2
Received Packets Discarded     = 4183
Received Packets Delivered     = 294396
Output Requests                = 287111
Routing Discards               = 0
Discarded Output Packets       = 28
Output Packet No Route        = 10
Reassembly Required            = 0
Reassembly Successful          = 0
Reassembly Failures           = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created              = 0

IPv6 Statistics

Packets Received                = 19826
Received Header Errors          = 0
Received Address Errors        = 47
Datagrams Forwarded            = 0
Unknown Protocols Received     = 0
Received Packets Discarded     = 2923
Received Packets Delivered     = 20433
Output Requests                = 21323
Routing Discards               = 0
Discarded Output Packets       = 11
Output Packet No Route        = 8
Reassembly Required            = 0
Reassembly Successful          = 0
Reassembly Failures           = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created              = 0

ICMPv4 Statistics

          Received      Sent
Messages      13         275
Errors         0           0
Destination Unreachable  7         269
Time Exceeded  2           0
Parameter Problems  0           0
Source Quenches  0           0
Redirects      0           0
Echo Replies   4           0
Echos         0           6
Timestamps    0           0
Timestamp Replies  0           0
    
```

هيووا شبکه

این سوئیچ وضعیت Offload را برای Connection های TCP نشان می دهد. این سوئیچ مربوط به Feature ایست با نام TCP Chimney Offload. به بیان ساده این Feature باعث می شود تا پردازش های Data مربوط به شبکه از CPU به کارت شبکه منتقل شود تا CPU آزادتر باشد. البته برای بهره برداری از این Feature باید کارت شبکه از این تکنولوژی Support کند. این تکنولوژی برای سرورهایی که به طور مداوم حجم زیادی از Data را مبادله می کنند مناسب است. البته استفاده از این تکنولوژی می تواند باعث بروز مشکلاتی هم بشود. قبل از استفاده از این تکنولوژی در مورد آن تحقیق کنید.

Netstat -t<

```

Administrator: Command Prompt
C:\Hiva>netstat -t
Active Connections

Proto Local Address           Foreign Address         State                   Offload State
-----
TCP    127.0.0.1:15485          activation:50418        ESTABLISHED            InHost
TCP    127.0.0.1:49177         activation:52001        ESTABLISHED            InHost
TCP    127.0.0.1:49178         activation:52001        ESTABLISHED            InHost
TCP    127.0.0.1:49179         activation:52001        ESTABLISHED            InHost
TCP    127.0.0.1:49180         activation:52001        ESTABLISHED            InHost
TCP    127.0.0.1:49729         activation:49730        ESTABLISHED            InHost
TCP    127.0.0.1:49730         activation:49729        ESTABLISHED            InHost
TCP    127.0.0.1:50418         activation:15485        ESTABLISHED            InHost
TCP    127.0.0.1:52001         activation:49177        ESTABLISHED            InHost
TCP    127.0.0.1:52001         activation:49178        ESTABLISHED            InHost
TCP    127.0.0.1:52001         activation:49179        ESTABLISHED            InHost
TCP    127.0.0.1:52001         activation:49180        ESTABLISHED            InHost
TCP    192.168.1.4:49760       ec2-52-24-201-104:https ESTABLISHED            InHost
TCP    192.168.1.4:50009       stackoverflow:https     ESTABLISHED            InHost
TCP    192.168.1.4:50419       ec2-54-164-220-52:https CLOSE_WAIT             InHost
TCP    192.168.1.4:50420       157.22.19.177:https    CLOSE_WAIT             InHost
TCP    192.168.1.4:50421       ec2-52-6-48-27:https   CLOSE_WAIT             InHost
TCP    192.168.1.4:50422       ec2-54-164-220-52:https CLOSE_WAIT             InHost
TCP    192.168.1.4:50423       ec2-52-6-48-27:https   CLOSE_WAIT             InHost
TCP    192.168.1.4:50424       ec2-52-6-48-27:https   CLOSE_WAIT             InHost

C:\Hiva>
    
```

همانطور که در تصویر بالا می بینید، با اجرای فرمان netstat -t ، یک ستون با نام Offload State افزوده می شود. اگر در قسمت State عبارت InHost نوشته شده باشد به معنای



Offload نشدن ترافیک شبکه است. اگر عبارت Offloaded نوشته شده باشد به معنای فعال بودن قابلیت TCP Chimney Offload است.

مشاهده وضعیت TCP Chimney Offload :

برای اطلاع از فعال یا غیر فعال بودن TCP Chimney Offload فرمان زیر را در خط فرمان وارد کنید:

```
netsh int tcp show global<
```

```
Administrator: Command Prompt
C:\Hiva>netsh int tcp show global
Querying active state...

TCP Global Parameters
-----
Receive-Side Scaling State      : enabled
Chimney Offload State           : disabled
NetDMA State                     : disabled
Direct Cache Access (DCA)      : disabled
Receive Window Auto-Tuning Level : normal
Add-On Congestion Control Provider : none
ECN Capability                   : disabled
RFC 1323 Timestamps            : disabled
Initial RTO                      : 3000
Receive Segment Coalescing State : disabled
Non Sack Rtt Resiliency         : disabled
Max SYN Retransmissions         : 2

C:\Hiva>
```

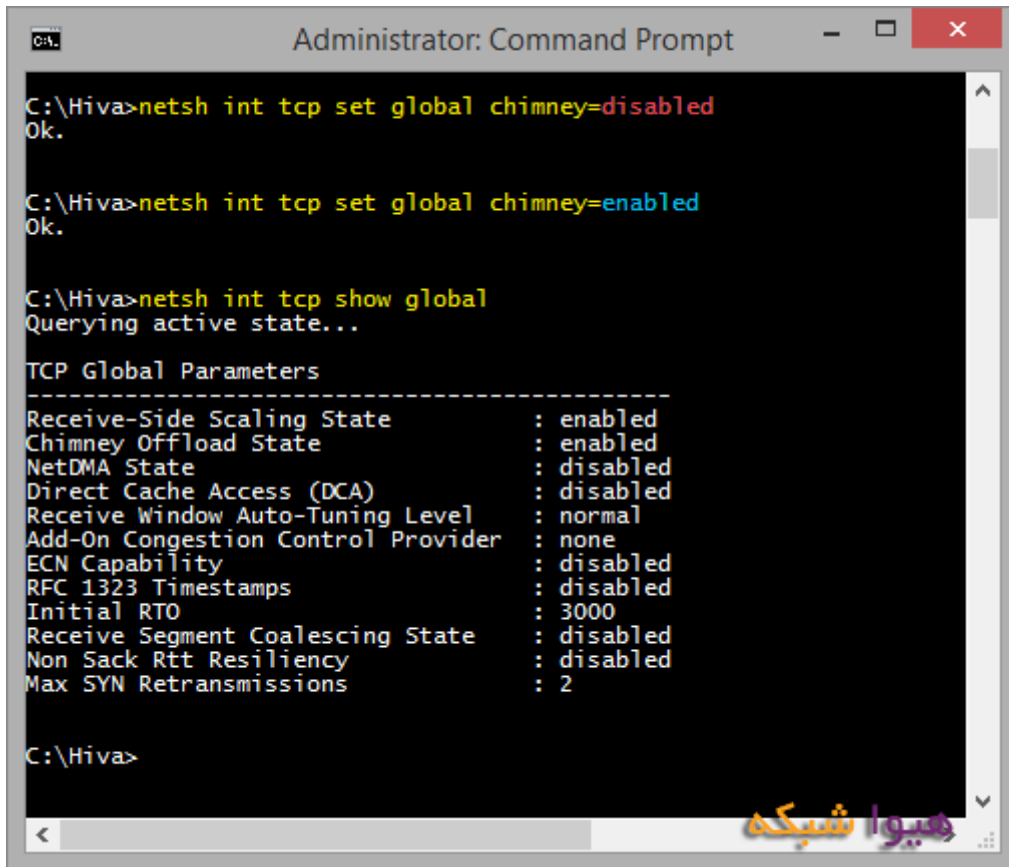
غیر فعال کردن TCP Chimney Offload :

```
netsh int tcp set global chimney=disabled<
```

فعال کردن TCP Chimney Offload :

```
netsh int tcp set global chimney=enabled<
```

پس از این فرمان اگر دوباره نگاهی به وضعیت TCP Chimney Offload بیاندازیم، می بینید که enable شده است:



```

Administrator: Command Prompt
C:\Hiva>netsh int tcp set global chimney=disabled
Ok.

C:\Hiva>netsh int tcp set global chimney=enabled
Ok.

C:\Hiva>netsh int tcp show global
Querying active state...

TCP Global Parameters
-----
Receive-Side Scaling State      : enabled
Chimney Offload State          : enabled
NetDMA State                    : disabled
Direct Cache Access (DCA)     : disabled
Receive Window Auto-Tuning Level : normal
Add-On Congestion Control Provider : none
ECN Capability                  : disabled
RFC 1323 Timestamps           : disabled
Initial RTO                     : 3000
Receive Segment Coalescing State : disabled
Non Sack Rtt Resiliency        : disabled
Max SYN Retransmissions        : 2

C:\Hiva>
  
```

Netstat -x

این سوئیچ به تازگی به ویندوز افزوده شده و در حال حاضر اطلاعات خاصی در مورد این Switch نیافتیم. پس از اجرای netstat -x در خط فرمان، به عنوان خروجی نیز اطلاعاتی نمایش داده نمی شود. این بخش در آینده تکمیل خواهد شد.

Netstat -y

این سوئیچ نیز مانند netstat -x به تازگی به افزوده شده اما بر خلاف netstat -x این فرمان خروجی دارد. این فرمان، Template مربوط به TCP Connection ها را نشان می دهد.

```

Administrator: Windows PowerShell
PS C:\Hiva> netstat -fy

Active Connections

Proto Local Address           Foreign Address         State           Template
----
TCP   127.0.0.1:15485         activation.cloud.techsmith.com:50035 ESTABLISHED    Internet
TCP   127.0.0.1:49209         activation.cloud.techsmith.com:52001 ESTABLISHED    Internet
TCP   127.0.0.1:49210         activation.cloud.techsmith.com:52001 ESTABLISHED    Internet
TCP   127.0.0.1:49211         activation.cloud.techsmith.com:52001 ESTABLISHED    Internet
TCP   127.0.0.1:49212         activation.cloud.techsmith.com:52001 ESTABLISHED    Internet
TCP   192.168.1.4:49819       a-0001.a-msedge.net:https ESTABLISHED    Internet
TCP   192.168.1.4:49820       a-0001.a-msedge.net:https ESTABLISHED    Internet
TCP   127.0.0.1:50035         activation.cloud.techsmith.com:15485 ESTABLISHED    Internet
TCP   192.168.1.4:50104       157.56.122.78:https    FIN_WAIT_2    Internet
TCP   127.0.0.1:52001         activation.cloud.techsmith.com:49210 ESTABLISHED    Internet
TCP   127.0.0.1:52001         activation.cloud.techsmith.com:49212 ESTABLISHED    Internet
TCP   127.0.0.1:52001         activation.cloud.techsmith.com:49209 ESTABLISHED    Internet
TCP   127.0.0.1:52001         activation.cloud.techsmith.com:49211 ESTABLISHED    Internet
PS C:\Hiva>
  
```

این بخش نیز در آینده کامل تر خواهد شد.

### Netstat interval

برای استفاده از فرمان Netstat در حالت Interval باید به جای عبارت Interval یک عدد وارد کنید که بیانگر "زمان بر حسب ثانیه" است. مثلا فرمان netstat -r 5 یعنی هر ۵ ثانیه فرمان netstat -r را اجرا کن. برای Stop کردن این وضعیت دکمه های Ctrl+C را فشار دهید.

امیدواریم این آموزش برای شما مفید واقع شده باشد.

گروه آموزشی هیوا شبکه