راهنمای

netstat

در سیستم عامل ویندوز

مرجع کامل

تالیف
مهندس هادی کیامرثی

تمام مثال های موجود در این مقاله با کامپیوتر تست شده اند تا از هر گونه خطا مبرا باشند با این حال ممکن است باز هم خطاهایی در آن وجود داشته باشد از کلیه خوانندگان این مقاله ، اساتید و دانشجویان محترم خواهشمندم برای مطلع کردن مولف از این خطا ها لطفا با ایمیل آدرس زیر تماس بگیرند

hadikiamarsi@gmail.com

در این مقاله مطالب زیر را خواهید آموخت

لیست کردن تمام ارتباطات و پورت های باز بوسیله نام آنها
لیست کردن تمام ارتباطات و پورت های باز بوسیله شماره آنها
لیست کردن ارتباطات یک پروتکل خاص و پورت های باز بوسیله نام آنها
لیست کردن تمام ارتباطات یک پروتکل خاص و پورت های باز بوسیله شماره آنها
نمایش همه ارتباطات به همراه شماره پروسه آن
نمایش همه ارتباطات به همراه شماره پروسه آن و آدرس نرم افزار ایجاد کننده آن
تکرار یک دستور به صورت پی در پی
نمایش جدول مسیریابی شبکه
نمایش مشخصات کامل هر پروتکل در شبکه
نمایش مشخصات کامل بسته های دریافتی و ارسالی و اشکالات شبکه

در هر شبکه ای دو مبحث اصلی وجود دارد اول نصب و پیکربندی شبکه دوم نگهداری و نظارت بر شبکه . نرم افزارهای زیادی برای نظارت بر شبکه وجود دارد که از این میان برخی رایگان و برخی پولی می باشند . از میان نرم افزارهای رایگان نظارت بر شبکه نرم افزار Netstat یکی از بهترین ها می باشد که به صورت پیش فرض همراه با سیستم عامل ویندوز نصب می شود و به راحتی در اختیار همه کاربران ویندوز می باشد . لازم به ذکر است که با وجود اینکه نرم افزار netstat رایگان می باشد ولی به لحاظ فنی و کاربرد از بسیاری از نرم افزار های تجاری بهتر و کامل تر می باشد . اگر شما یک متخصص شبکه یا متخصص امنیت شبکه می باشید آشنایی با این ابزار برای شما از واجبات می باشد . برای بررسی مثال های این مقاله از جدول های زیر استفاده نمایید .

جدول شماره یک

ردیف	نام	توضیحات
1	Proto	نام پرتکل را نشان می دهد
2	Local Address	آی پی آدرس مبدا را نشان می دهد
3	Foreign Address	آی پی آدرس مقصد را نشان می دهد
4	State	وضعیت ارتباط را نشان می دهد
5	PID	نام پروسه نرم افزار ایجاد کننده ارتباط را نشان می دهد

جدول شماره دو

ردیف	نام	توضیحات
1	IP	نام نوعی پروتکل
2	IPv6	نام نوعی پروتکل
3	ICMP	نام نوعی پروتکل
4	ICMPv6	نام نوعی پروتکل
5	TCP	نام نوعی پروتکل
6	TCPv6	نام نوعی پروتکل
7	UDP	نام نوعی پروتکل
8	UDPv6	نام نوعی پروتکل

جدول شماره سه

ردیف	نام سوئیچ	توضیحات
1	-a	همه ارتباطات را نشان می دهد
2	-b	آدرس نرم افزار ایجاد کننده ارتباط را نمایش می دهد
3	-e	گزارش کاملی از بایت

4	-n	پورت و آی پی آدرس ها را به صورت عددی نمایش می دهد
5	-o	شماره پروسه نرم افزار ایجاد کننده ارتباط را نشان می دهد
6	-p	بوسیله این سوییچ می توانید نوع پروتکل مورد نظر را تعیین نمایید
7	-r	جدول مسیریابی را نمایش می دهد
8	-s	گزارش کاملی از دریافت بسته ها و اشکالات در تمام پروتکل های شبکه نمایش می دهد
9	-v	لیست کامپوننت های مرتبط با فایل ایجاد کننده اتباط را به ترتیب نمایش می دهد
10	Interval	باعث می شود دستوری که صادر کردید هر چند ثانیه تکرار گردد و باید برای متوقف کردن آن از کلید های CTRL + C استفاده نمایید

لیست کردن تمام ارتباطات و پورت های باز بوسیله نام آنها

```
Netstat –a
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود برای بررسی نتیجه به جدول شماره یک مراجعه نمایید

```
Proto  Local Address          Foreign Address        State
```

```
TCP    unknown-dfc42d2:epmap  0.0.0.0:0              LISTENING
TCP    unknown-dfc42d2:microsoft-ds  0.0.0.0:0            LISTENING
TCP    unknown-dfc42d2:ms-wbt-server  0.0.0.0:0            LISTENING
TCP    unknown-dfc42d2:1025   0.0.0.0:0              LISTENING
UDP    unknown-dfc42d2:microsoft-ds  *:*
UDP    unknown-dfc42d2:isakmp  *:*
UDP    unknown-dfc42d2:ipsec-msft  *:*
UDP    unknown-dfc42d2:ntp    *:*
UDP    unknown-dfc42d2:ssdp   *:*
```

لیست کردن تمام ارتباطات و پورت های باز بوسیله شماره آنها

```
Netstat –an
Netstat –a –n
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
Proto  Local Address          Foreign Address        State
 TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
 TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
 TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
 TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
 UDP    0.0.0.0:445            *:*
 UDP    0.0.0.0:500            *:*
 UDP    0.0.0.0:4500           *:*
 UDP    127.0.0.1:123          *:*
 UDP    127.0.0.1:1900         *:*
```

لیست کردن ارتباطات یک پروتکل خاص و پورت های باز بوسیله نام آنها

برای دسترسی به لیست پروتکل های قابل پشتیبانی در دستور زیر به جدول شماره دو مراجعه نمایید

```
Netstat –p tcp –a
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    unknown-dfc42d2:epmap  0.0.0.0:0              LISTENING
```

```
  TCP    unknown-dfc42d2:microsoft-ds  0.0.0.0:0              LISTENING
  TCP    unknown-dfc42d2:ms-wbt-server  0.0.0.0:0            LISTENING
  TCP    unknown-dfc42d2:1025   0.0.0.0:0              LISTENING
```

لیست کردن تمام ارتباطات یک پروتکل خاص و پورت های باز بوسیله شماره آنها

```
Netstat –p tcp –na
Netstat –p tcp –n –a
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
```

نمایش همه ارتباطات به همراه شماره پروسه آن

```
Netstat –ao
Netstat –a –o
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    unknown-dfc42d2:epmap  0.0.0.0:0              LISTENING       852
  TCP    unknown-dfc42d2:microsoft-ds  0.0.0.0:0              LISTENING       4
  TCP    unknown-dfc42d2:ms-wbt-server  0.0.0.0:0              LISTENING       8
08
  TCP    unknown-dfc42d2:1025   0.0.0.0:0              LISTENING       1816
  UDP    unknown-dfc42d2:microsoft-ds  *:*                                    4
  UDP    unknown-dfc42d2:isakmp  *:*                                    656
```

```
 UDP    unknown-dfc42d2:ipsec-msft  *:*                    656
 UDP    unknown-dfc42d2:ntp    *:*                    892
 UDP    unknown-dfc42d2:ssdp   *:*                    1080
```

نمایش همه ارتباطات به همراه شماره پروسه آن و آدرس نرم افزار ایجاد کننده آن

```
Netstat –ab
Netstat –a –b
Netstat –abv
Netstat –a –b -v
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
UDP    unknown-dfc42d2:microsoft-ds  *:*
 [System]

 UDP    unknown-dfc42d2:ipsec-msft  *:*                    65
[lsass.exe]

 UDP    unknown-dfc42d2:isakmp  *:*                    656
[lsass.exe]

 UDP    unknown-dfc42d2:ssdp   *:*                    1080
c:\windows\system32\WS2_32.dll
c:\windows\system32\ssdpsrv.dll
C:\WINDOWS\system32\ADVAPI32.dll
C:\WINDOWS\system32\kernel32.dll
[svchost.exe]

 UDP    unknown-dfc42d2:ntp    *:*                    892
c:\windows\system32\WS2_32.dll
c:\windows\system32\w32time.dll
ntdll.dll
C:\WINDOWS\system32\kernel32.dll
[svchost.exe]
```

تکرار یک دستور به صورت پی در پی

```
Netstat –na 1
Netstat –na 3
Netstat –n –a 5
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1025         0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1900         *:*
```

نمایش جدول مسیریابی شبکه

```
Netstat –r
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 90 f5 39 25 98 ...... Realtek RTL8139/810x Family Fast Ethernet NIC
Packet Scheduler Miniport
===========================================================================
```

```
===========================================================
===========================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
    255.255.255.255  255.255.255.255  255.255.255.255             2       1
===========================================================
===========================
Persistent Routes:
  None
```

نمایش مشخصات کامل هر پروتکل در شبکه

```
Netstat –s
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
TCP Statistics for IPv4

  Active Opens                        = 0
  Passive Opens                       = 0
  Failed Connection Attempts          = 0
  Reset Connections                   = 0
  Current Connections                 = 0
  Segments Received                   = 0
  Segments Sent                       = 0
  Segments Retransmitted              = 0

UDP Statistics for IPv4

  Datagrams Received    = 4
  No Ports              = 0
  Receive Errors        = 0
  Datagrams Sent        = 4
```

نمایش مشخصات کامل بسته های دریافتی و ارسالی و اشکالات شبکه

```
Netstat –e
```

دستور بالا نتیجه مانند زیر ظاهر خواهد نمود

```
Interface Statistics
```

	Received	Sent
Bytes	512	512
Unicast packets	4	4
Non-unicast packets	0	1
Discards	0	0
Errors	0	0
Unknown protocols	0	

این گزینه را به s– نیز می توان بکاربرد

```
Netstat –es
Netstat –e -s
```