

**Not quite what you are looking for? You may want to try:**

- [Getting active TCP/UDP connections on a box](#)
- [The Quick and Easy Way to Add Web Interfaces to C/C++ Applications](#)

[highlights off](#)

7,772,759 members and growing! (32,497 online)

lubita7052 290 [Sign out](#)[Home](#) [Articles](#) [Questions & Answers](#)[Learning Zones](#) [Features](#) [Help!](#) [The Lounge](#)[Home](#) » [General Programming](#) » [Internet / Network](#) » [General](#)

Enhance netstat

Licence
First Posted **16 Nov 2003**
Views **90,080**
Downloads **2,082**
Bookmarked **32 times**

See Also

- [More like this](#)
- [More by this author](#)

By [y0da](#) | 16 Nov 2003[VC6](#) [VC7](#) [VC7.1](#) [Win2K](#) [WinXP](#) [Win2003](#) [MFC](#) [Dev](#) [Intermediate](#)

This article shows an implementation of the main TCP/UDP functions of the IP Helper API that is used to get info about active connections including the process attached to a connection.

Article	Browse Code	Stats	Revisions	28			
3.78 (10 votes)							

Sponsored Links

Is your email address OK? You are signed up for our newsletters but your email address is either unconfirmed, or has not been reconfirmed in a long time. Please click [here](#) to have a confirmation email sent so we can confirm your email address and start sending you newsletters again. Alternatively, you can [update your subscriptions](#).

[Download source files - 11.7 Kb](#)[Download demo project - 105 Kb](#)

```

C:\WINNT\System32\cmd.exe
D:\Enetstat\Release>netstat /e

Proto Local Address          Local Port   Remote Address      Remote Port   Connection State
TCP    127.0.0.1                1027        127.0.0.1           1035         ESTAB
TCP    127.0.0.1                1035        127.0.0.1           1027         ESTAB
TCP    127.0.0.1                1157        127.0.0.1           1158         ESTAB
TCP    127.0.0.1                1158        127.0.0.1           1157         ESTAB
TCP    127.0.0.1                3163        127.0.0.1           3164         ESTAB
TCP    127.0.0.1                3164        127.0.0.1           3163         ESTAB
TCP    163.242.237.192         1029        163.242.244.96      139          ESTAB
TCP    163.242.237.192         1030        163.242.245.3       139          ESTAB
TCP    163.242.237.192         1132        163.242.244.17      1074         ESTAB
TCP    163.242.237.192         1135        163.242.244.17      1074         ESTAB
TCP    163.242.237.192         1139        163.242.244.17      1098         ESTAB
TCP    163.242.237.192         1143        163.242.244.17      1098         ESTAB
TCP    163.242.237.192         1160        163.242.237.192     1194         ESTAB
TCP    163.242.237.192         1184        163.242.244.218     139          ESTAB
TCP    163.242.237.192         1194        163.242.237.192     1160         ESTAB
TCP    163.242.237.192         2887        163.242.244.218     44299        ESTAB
TCP    163.242.237.192         2888        163.242.244.218     48245        ESTAB
TCP    163.242.237.192         2890        163.242.244.16      23           ESTAB
TCP    163.242.237.192         4491        163.242.244.16      139          ESTAB

D:\Enetstat\Release>netstat /k 163.242.244.16 2890
Connection closed succesfully ;>

Proto Local Address          Local Port   Remote Address      Remote Port   Connection State
TCP    127.0.0.1                1027        127.0.0.1           1035         ESTAB
TCP    127.0.0.1                1035        127.0.0.1           1027         ESTAB
TCP    127.0.0.1                1157        127.0.0.1           1158         ESTAB
TCP    127.0.0.1                1158        127.0.0.1           1157         ESTAB
TCP    127.0.0.1                3163        127.0.0.1           3164         ESTAB
TCP    127.0.0.1                3164        127.0.0.1           3163         ESTAB
TCP    163.242.237.192         1029        163.242.244.96      139          ESTAB
TCP    163.242.237.192         1030        163.242.245.3       139          ESTAB
TCP    163.242.237.192         1132        163.242.244.17      1074         ESTAB
TCP    163.242.237.192         1135        163.242.244.17      1074         ESTAB
TCP    163.242.237.192         1139        163.242.244.17      1098         ESTAB
TCP    163.242.237.192         1143        163.242.244.17      1098         ESTAB
TCP    163.242.237.192         1160        163.242.237.192     1194         ESTAB
TCP    163.242.237.192         1184        163.242.244.218     139          ESTAB
TCP    163.242.237.192         1194        163.242.237.192     1160         ESTAB
TCP    163.242.237.192         2887        163.242.244.218     44299        ESTAB
TCP    163.242.237.192         2888        163.242.244.218     48245        ESTAB
TCP    163.242.237.192         2891        163.242.244.218     48821        ESTAB
TCP    163.242.237.192         4491        163.242.244.16      139          ESTAB

```

Introduction

The main idea of this project was already implemented and presented by some guys around here: using [GetTcpTable](#) and [GetUdpTable](#) to read connection states of running processes. Yet another thing that is mentioned in this kind of articles are two undocumented APIs from *iphlpapi.dll*: [AllocateAndGetTcpExTableFromStack](#) and [AllocateAndGetUdpExTableFromStack](#). Using these APIs, we can get access to the name of the process that holds the running connection. Unfortunately it does work only with Win2000, WinXP or newer versions.

Description

First of all, I'd like to mention there is something new regarding this subject. [Enetstat](#) will allow the user to close any "established" connection using the following API function:

[Collapse](#) | [Copy Code](#)

```

DWORD SetTcpEntry(
    PMIB_TCPCROW pTcpRow
);

```

Having an established connection, we can close it using the following state: [MIB_TCP_STATE_DELETE_TCB](#).

[Collapse](#) | [Copy Code](#)

```
MIB_TCPROW sKillConn;  
sKillConn.dwLocalAddr = (DWORD)ulLocIP; //local ip  
sKillConn.dwLocalPort = (DWORD)usLocalPort; //local  
port  
sKillConn.dwRemoteAddr = (DWORD)ulRemIP; //remote ip  
sKillConn.dwRemotePort = (DWORD)usRemPort; //remote  
port  
sKillConn.dwState = MIB_TCP_STATE_DELETE_TCB;  
  
DWORD dwRez = SetTcpEntry(&sKillConn);
```

That's all about it. My piece of code is not described in detail and I suppose there is no need for that as long as we already have a cool and detailed description made by [Axel Charpentier](#).

Well, if you need any good reference about this subject you'll find it here:

[Getting active TCP/UDP connections on a box](#), by [Axel Charpentier](#).

License

This article has no explicit license attached to it but may contain usage terms in the article text or the download files themselves. If in doubt please contact the author via the discussion board below.

A list of licenses authors might use can be found [here](#)

About the Author

y0da



Web Developer

 Romania

Member

[Article Top](#) **Rate this article for us!** Poor ☐ ☐ ☐ ☐ ☐ Excellent [Vote](#)























Comments and Discussions








FAQ

Noise Tolerance Layout Per
page

New Message Msgs 1 to 25 of 28 (Total in Forum: 28) (Refresh) First Prev Next

Always 87!!! eRRaTuM	7:18 16 Mar '08
Not in 2000, deprecated in Vista Idsandon	3:44 6 Dec '06
Re: Not in 2000, deprecated in Vista y0da	4:01 6 Dec '06
Re: Not in 2000, deprecated in Vista Leo Davidson	4:48 28 Mar '09
printer Kutti Ra	18:59 30 Sep '05
Monitoring Internet client Kutti Ra	18:56 30 Sep '05
TcpTable does not return all connections bigga	7:16 16 Sep '05
Re: TcpTable does not return all connections y0da	7:32 16 Sep '05
What about speed ? Smart K8	0:29 6 Feb '05
Re: What about speed ? y0da	1:25 6 Feb '05
Re: What about speed ? Smart K8	1:18 7 Feb '05
stack Memory Leak mervick	18:43 26 Jan '05
Re: stack Memory Leak y0da	23:22 26 Jan '05
Re: stack Memory Leak mervick	18:17 27 Jan '05
Re: stack Memory Leak y0da	23:19 27 Jan '05
enetstat on winnt and Win2k and NT4 y0da	23:25 27 Apr '04

	AllocateAndGetTcpExTableFromStack for Windows 2000 	 blakeo23	11:39 14 Apr '04
	Re: AllocateAndGetTcpExTableFromStack for Windows 2000 	 Anonymous	23:01 14 Apr '04
	Re: AllocateAndGetTcpExTableFromStack for Windows 2000 	 blakeo23	3:10 15 Apr '04
	How to close UDP ports ? 	 marcosvelasco	8:21 16 Dec '03
	Re: How to close UDP ports ? 	 Anonymous	13:29 19 Dec '03
	A free tool called Active Ports can work under Windows 2K 	 Johannowic	22:25 19 Nov '03
	Re: A free tool called Active Ports can work under Windows 2K 	 y0da	3:30 20 Nov '03
	Windows 2000 and XP... 	 marcosvelasco	10:00 18 Nov '03
	Re: Windows 2000 and XP... 	 y0da	3:10 19 Nov '03
Last Visit: 17:49 4 May '11 Last Update: 7:50 7 May '11 1 2 Next »			

 General
  News
  Question
  Answer
  Joke
  Rant
  Admin

Use Ctrl+Left/Right to switch messages, Ctrl+Up/Down to switch threads, Ctrl+PgUp/PgDown to switch pages.

[link](#) | [Privacy](#) | [Terms of Use](#) | [Mobile](#)

Last Updated: 16 Nov 2003

Copyright 2003 by y0da
 Everything else Copyright © [CodeProject](#),
 1999-2011

Web21 | [Advertise on the Code Project](#)

Spread for ASP.NET

FarPoint Spread for ASP.NET 5 by GrapeCity is...

www.gcpowertools.com

Get 6 Months Free ASP.NET Hosting!

DiscountASP.NET is a Microsoft Windows-based...

www.discountasp.net

Data Dynamics Reports for Windows Forms, ASP.NET

Data Dynamics Reports for Business Reporting...

www.gcpowertools.com

See Also...

[Windows netstat application](#)

Windows netstat application.

[Getting active TCP/UDP connections on a box](#)

This article shows an implementation of the...

[EnetstatX](#)

Enhance netstat and packet filtering.

[Getting the active TCP/UDP connections using the GetExtendedTcpTable function](#)

This article shows how to use some TCP/UDP...

[Applications Traffic Watcher](#)

Applications Traffic Watcher is a small...

The Daily Insider

[30 free programming books](#)

Daily News: [Signup now](#).