<https://www.cnblogs.com/xxcanghai/p/4958577.html>

该博客还有更多的批处理教程

# [批处理]NetstatFilter快速查找端口被占用问题](https://www.cnblogs.com/xxcanghai/p/4958577.html)

* [前言](javascript:;)
* [使用方法](javascript:;)
* [如何看懂显示列表](javascript:;)
  + [什么是netstat命令？](javascript:;)
  + [什么是PID？](javascript:;)
  + [“状态”字段有哪些类型及含义？](javascript:;)
  + [什么是本地地址，外部地址？](javascript:;)
* [查询某进程占用的端口号](javascript:;)
* [查询某端口被哪个进程所占用](javascript:;)
* [程序源码下载](javascript:;)

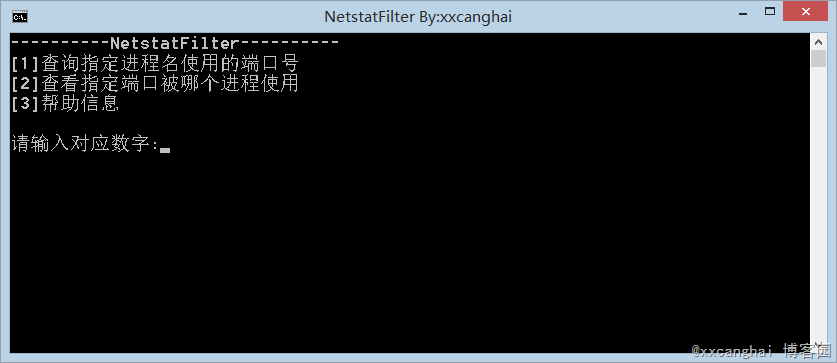
前言

准确的说，他是一个网络连接端口查看器，可以根据进程查端口，也可以根据端口查进程。期初是因在使用Fiddler的时候发现无法启动，提示端口被占用，但是由不知道用什么方法才能找到是哪个程序占用的Fiddler的端口，遂使用命令行的netstat命令配合find命令才找到，遂想写这样一个类似的工具帮助我们速度定位类似端口问题的所在。

PS：可预见很多人会说为什么不用360网络链接查看器，或是其他类似软件，功能更强大界面更美观巴拉巴拉…？

答：因为我喜欢bat批处理，我喜欢命令行，喜欢能用几句命令搞定的事就不用一个别的软件来搞，更重要的是享受编写代码这其中的过程。

使用方法

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161331369-775153481.png)

主要功能就两个：

1、查询某个进程都在使用哪些端口号，包含同进程名的所有实例，以及他们分别所占用的TCP和UDP端口。

2、查看某个端口被哪个进程使用，包括远程IP和本地IP，以及TCP和UDP的所有端口

如何看懂显示列表

程序界面：

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161332259-508124145.png)

本程序返回值使用的windows命令行下的**netstat**命令。

什么是netstat命令？

Netstat，在Internet RFC标准中，Netstat的定义是： Netstat是在内核中访问网络及相关信息的程序，它能提供TCP连接，TCP和UDP监听，进程内存管理的相关报告。

具体的关于netstat命令的用法可以参见：[netstat百度百科](http://baike.baidu.com/link?url=IRSfEB3X8CUGq-DgbUEgwqFG8BFpQT2NPnjEBjgPZTgLo71Ty27n7EROUxXG-2ixs_jUIL8_HbIqA-XRlfnmJa" \t "_blank)，[WIKI](https://en.wikipedia.org/wiki/Netstat)，[如何用netstat命令查看端口占用问题](http://www.3lian.com/edu/2013/08-03/86406.html" \t "_blank)等

什么是PID？

PID（ProcessID）操作系统里指进程ID号。操作系统里每打开一个程序都会创建一个进程ID，即PID。  
PID就是各进程的身份标识，程序一运行系统就会自动分配给进程一个独一无二的PID。进程中止后PID被系统回收，可能会被继续分配给新运行的程序。  
PID一列代表了各进程的进程ID，也就是说，PID就是各进程的身份标识。

“状态”字段有哪些类型及含义？

连接状态。在原模式中没有状态，在用户数据报协议中也经常没有状态，于是状态列可以空出来。若有状态，通常取值为：  
LISTEN  
侦听来自远方的TCP端口的连接请求  
SYN-SENT  
在发送连接请求后等待匹配的连接请求  
SYN-RECEIVED  
在收到和发送一个连接请求后等待对方对连接请求的确   
ESTABLISHED  
代表一个打开的连接  
FIN-WAIT-1  
等待远程TCP连接中断请求，或先前的连接中断请求的确认  
FIN-WAIT-2  
从远程TCP等待连接中断请求  
CLOSE-WAIT  
等待从本地用户发来的连接中断请求  
CLOSING  
等待远程TCP对连接中断的确认  
LAST-ACK  
等待原来的发向远程TCP的连接中断请求的确认  
TIME-WAIT  
等待足够的时间以确保远程TCP接收到连接中断请求的确认

CLOSED  
没有任何连接状态

什么是本地地址，外部地址？

简单的讲，本地地址即当前这个链接到你本机通信的IP地址和端口，外部地址即当前这个链接到的远程服务器地址和端口。

当然本地和外部地址都有可能是本地地址，一般端口不一样而已。一个典型的应用就是代理服务软件

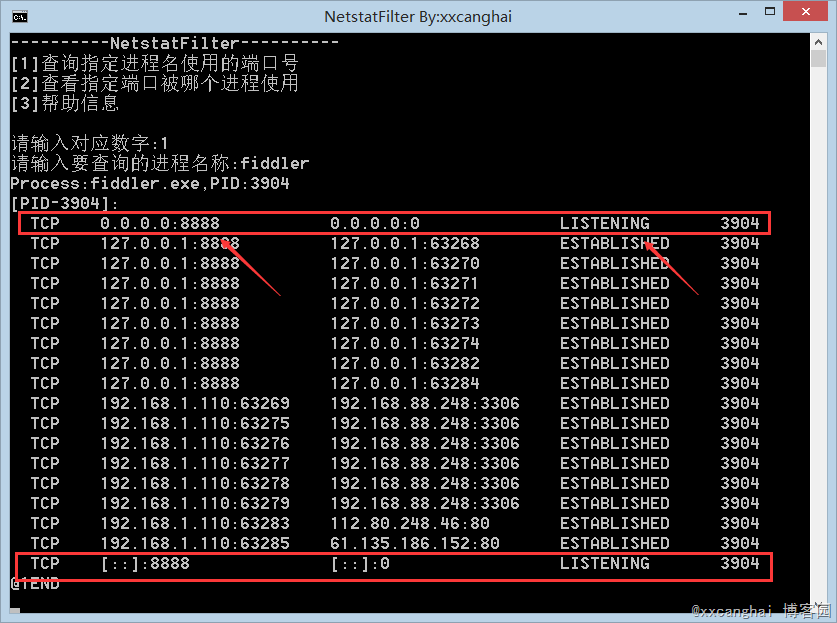
具体的可以参见：[端口百科](http://baike.baidu.com/view/1075.htm" \t "_blank) 中相关地址的解释，或是参见：[NAT概念中的四类地址概念](http://blog.chinaunix.net/uid-62554-id-2720909.html" \t "_blank)，也有助于理解。

查询某进程占用的端口号

这里我们查询Fiddler.exe所占用的端口号，在主界面选择1，回车。再输入Fiddler回车

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161332994-1551937357.png)

可以看到红框内，Fiddler占用了本地IPv4和IPv6的8888端口，并且一直处于监听（LISTENING）状态。

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161333744-365569743.png)

注意：最后一行的[::]表示IPv6的所有地址，等同于IPv4的0.0.0.0地址

此地址在不同环境有不同名称，若在路由表中他表示默认路由。在网络编程中，若监听此地址的端口，则可相当于同时监听本地回环地址127.0.0.1以及localhost地址以及本机所有网卡的本地地址（如192.168.1.100）的端口。

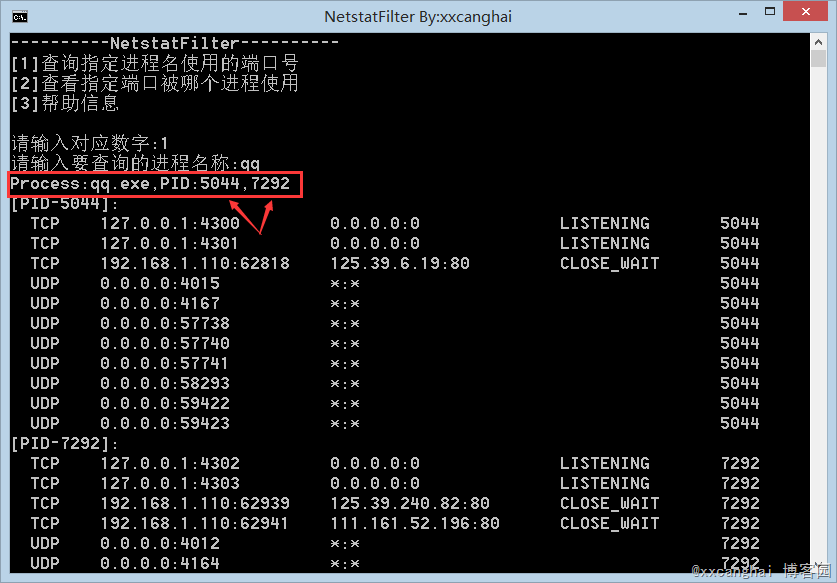
反之，若只监听当前网卡本地地址192.168.1.100的端口，则使用127.0.0.1地址就访问不到

关于什么是0.0.0.0地址可以参考：[WIKI](https://en.wikipedia.org/wiki/0.0.0.0" \t "_blank)，[这里](http://www.cnblogs.com/hnrainll/archive/2011/10/13/2210101.html" \t "_blank)

关于0.0.0.0和127.0.0.1的区别可以参考：[红黑](http://www.2cto.com/net/201310/253427.html" \t "_blank)，[文库](http://wenku.baidu.com/link?url=FudFFKrEByOzUqy33zA5dSJCKKFAJ5fapd_u8u0xu6Yl8zsuLznDnOBH3GeTaXTmeI27WIGhi8mTBLi8cuFC_laBI92kPiu71uZsGu5SrIi)，[stackoverflow](http://stackoverflow.com/questions/20778771/what-is-the-difference-between-0-0-0-0-127-0-0-1-and-localhost)，以及 [知乎的讨论](http://www.zhihu.com/question/23940717)等

好了扯远了，继续说bat用法，看到本地全零地址，以及监听状态，就可以判断此程序Fiddler在占用8888端口，此时若有其他程序如IIS，汤姆猫之类的程序要启动同端口就会报错了。

再看看QQ的占用情况：

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161334962-993228801.png)

可以看到当前有两个进程叫QQ.exe，他们的分别的链接情况及TCP、UDP链接如图所示。

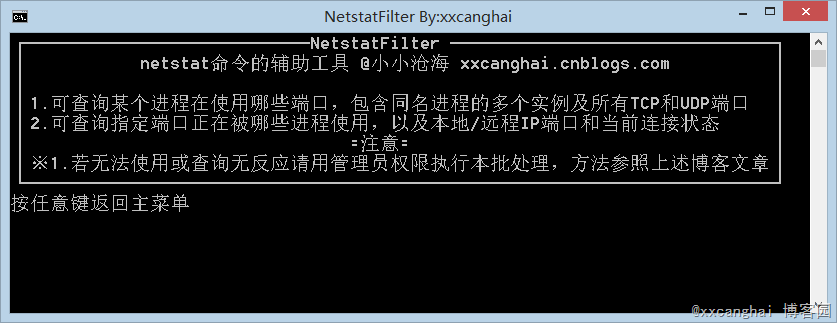
查询某端口被哪个进程所占用

这里我们依旧测试Fiddler的8888端口，这里输入2回车，输入端口号8888回车，查看结果：

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161335775-421266594.png)

可以看到8888端口在IPv4和IPv6上都由Fiddler.exe在占用（监听）

帮助信息：

[](http://images2015.cnblogs.com/blog/746158/201511/746158-20151112161338915-1800854469.png)

注意：若无法使用或查询无响应，请使用管理员权限启用本批处理，方法可以参照我之前写的文章：[如何创建管理员权限的CMD命令提示符窗口](http://www.cnblogs.com/xxcanghai/p/4610054.html)

程序源码下载

源码已经托管至Github：

[https://github.com/xxcanghai/cnblogsFiles/blob/master/NetstatFilter网络连接查看器.bat](https://github.com/xxcanghai/cnblogsFiles/blob/master/NetstatFilter%E7%BD%91%E7%BB%9C%E8%BF%9E%E6%8E%A5%E6%9F%A5%E7%9C%8B%E5%99%A8.bat)

或是直接复制下述所有代码保存到.bat文件后，直接运行即可。

批处理代码：

[复制代码](javascript:void(0);)

::NetstatFilter网络连接查看器 @小小沧海 xxcanghai.cnblogs.com By:2015年6月29日

@echo off

:start

title NetstatFilter By:xxcanghai

SETLOCAL ENABLEEXTENSIONS&SETLOCAL ENABLEDELAYEDEXPANSION

cls

::######config######

set PCENAME=

set PID=

set PORT=

::inner config

set ERRORCODE=0

:menu

cls&echo ----------NetstatFilter----------

echo [1]查询指定进程名使用的端口号

echo [2]查看指定端口被哪个进程使用

echo [3]帮助信息

echo.

set /p=请输入对应数字:<nul

set select=3&set /p select=

if /i "%select%"=="q" exit /b

if /i "%select%"=="exit" exit /b

if "%select%"=="1" goto :menuitem1

if "%select%"=="2" goto :menuitem2

if "%select%"=="3" goto :help

cls&goto :menu

:menuitem1

set /p=请输入要查询的进程名称:<nul

set PCENAME=&set /p PCENAME=

if /i "%PCENAME%"=="q" goto :menu

if "%PCENAME%"=="" goto :menuitem1

if "%PCENAME:.=%"=="%PCENAME%" set PCENAME=%PCENAME%.exe

call :getpid "%PCENAME%" PID

echo Process:%PCENAME%,PID:%PID%

call :getnetbypid "%PID%"

echo @1END&pause>nul&goto start

:menuitem2

set /p=请输入要查询的端口号:<nul

set PORT=&set/p PORT=

if /i "%PORT%"=="q" goto :menu

if "%PORT%"=="" goto :menuitem2

call :getnetbyport "%PORT%"

echo @2END&pause>nul&goto start

:help

cls

echo ┏━━━━━━━━━━━━━━NetstatFilter ━━━━━━━━━━━━━━━━┓

echo ┃ netstat命令的辅助工具 @小小沧海 xxcanghai.cnblogs.com ┃

echo ┃ ┃

echo ┃1.可查询某个进程在使用哪些端口，包含同名进程的多个实例及所有TCP和UDP端口 ┃

echo ┃2.可查询指定端口正在被哪些进程使用，以及本地/远程IP端口和当前连接状态 ┃

echo ┃ =注意= ┃

echo ┃※1.若无法使用或查询无反应请用管理员权限执行本批处理，方法参照上述博客文章┃

echo ┗━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━┛

echo 按任意键返回主菜单&pause>nul&goto start

::#####get pid by process#####

::[tasklist] example

::cmd.exe 11132 Console 1 3,000 K

::cmd.exe 8204 Console 1 2,728 K

::cmd.exe 10060 Console 1 2,996 K

:getpid

if not "%~1"=="" (

set PID=

for /f "tokens=2 delims= " %%i in ('tasklist /fi "imagename eq %~1" /nh /fo table^|find /i "%~1"') do (

set PID=!PID!%%i,

)

if "!PID!"=="" (

set ERRORCODE=101

echo [ERROR]ProcessName "%~1" is not found

pause>nul&goto start

) else (

set PID=!PID:~0,-1!

)

set %2=!PID!

goto :eof

)

::#####get netstat by pid#####

::[netstat] example:

:: Proto Local Address Foreign Address State PID

:: TCP 0.0.0.0:80 0.0.0.0:0 LISTENING 4

:: UDP [::1]:50575 \*:\* 5108

:getnetbypid

if not "%~1"=="" (

set PID=%~1

for /f "tokens=1,\* delims=," %%a in ("!PID!") do (

set subpid=%%a

set PID=%%b

::get TCP

echo [PID-!subpid!]:

for /f "delims=" %%z in ('netstat -a -n -o^|find ":"') do (

set tLine=%%z

::netstat的IPv6结果中含有%符号，%符号在call传递中会发生错误，遂将%替换为$后再传递

set tLine=!tLine:%%=$!

call :getNetInfo "!tLine!" tProto tLocalAdd tForeignAdd tState tPID

set tLine=!tLine:$=%%!

::call使用完成后将$符号替换回%符号

if "!tPID!"=="!subpid!" (

echo !tLine!

)

)

)

if not "!PID!"=="" (call %0 "!PID!")

goto :eof

)

::#####get netstat by port#####

:getnetbyport

if not "%~1"=="" (

set PORT=%~1

for /f "tokens=1,\* delims=," %%a in ("!PORT!") do (

set myport=%%a

set PORT=%%b

::PORT==8888

for /f "delims=" %%z in ('netstat -a -n -o^|find /i ":!myport! "') do (

set tLine=%%z

set tLine=!tLine:%%=$!

call :getNetInfo "!tLine!" tProto tLocalAdd tForeignAdd tState tPID

set tLine=!tLine:$=%%!

echo !tLine!

for /f "tokens=1 delims= " %%j in ('tasklist /nh /fi "PID eq !tPID!"') do (

echo [%%j]

)

)

)

)

goto :eof

echo END.&pause>nul&goto start

exit

::#####FUNCTION#####

:getNetInfo

::将netstat -ano的某一行分隔成不同的变量

::call :getNetInfo "<netstat output line>" tProto tLocalAdd tForeignAdd tState tPID

if not "%~1"=="" (

for /f "tokens=1,2,3,4,5 delims= " %%i in ("%~1") do (

set %2=%%i

set %3=%%j

set %4=%%k

if "%%i"=="TCP" (

set %5=%%l

set %6=%%m

) else (

set %5=

set %6=%%l

)

)

)

goto :eof

::#####FUNCTION#####

:split

::%0为函数名称自身:split，%1为传过来的值,%~1为删除变量中的双引号"

::在此子搜索函数中把过滤器按照/符号分割开，并取得分割后的第一个的值

::再把分割后的剩下的值重赋予过滤器，并调用自身，直到过滤器为空为止，返回

set subf=%~1

for /f "tokens=1,\* delims=," %%j in ("%subf%") do (

set subf=%%k

)

if not "!subf!"=="" (call %0 "!subf!")

goto :eof

::#####FUNCTION#####

:FUN1

goto :eof

[复制代码](javascript:void(0);)

**原文地址-小小沧海：http://www.cnblogs.com/xxcanghai/p/4958577.html**

**如果您认为本文对得起您所阅读他所花的时间，欢迎点击右下角↘ 推荐。您的支持是我继续写作最大的动力，谢谢**

作者：[小小沧海](http://www.cnblogs.com/xxcanghai/)   
出处：<http://www.cnblogs.com/xxcanghai/>   
本文地址：<http://www.cnblogs.com/xxcanghai/>   
本文版权归作者和博客园共有，欢迎转载，但未经作者同意必须保留此段声明，且在文章页面明显位置给出原文连接，否则保留追究法律责任的权利。

分类: [BAT批处理](https://www.cnblogs.com/xxcanghai/category/701938.html)

标签: [批处理 bat](https://www.cnblogs.com/xxcanghai/tag/%E6%89%B9%E5%A4%84%E7%90%86%20bat/)