

# 觀察你電腦的上的網路連線狀態及程序(netstat)

張明泰 (mtchang.tw@gmail.com)

**netstat** 是一個可以查詢本機網路和外界網路連線的指令，可以透過這個指令的查詢得知有沒有奇怪的連線在你的機器中連線，也可透過此指令瞭解電腦連線的狀況。這個指令 **windows** 上也有，**Linux** 上也有，但在參數與用法有一些不同。

**Windows** 上得說明可以參考 **MS** 公司的 **netstat** 說明

(<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netstat.mspx?mfr=true>)

節錄及翻譯如下：

語法：

**netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]**

參數：

**-a**：顯示所有活動中的 **TCP** 連線，及 **TCP and UDP ports** 上聆聽中的資訊。

**-e**：顯示網路的統計資訊，如 **bytes** 數和封包發送和接收的數量。這參數通常和 **-s** 並用。

**-n**：顯示活動的 **TCP** 連線，但是 **ip address** 和 **port** 編號沒有被解釋翻譯成為名稱說明。(通常可以加速顯示的速度因為反解通常需要查詢 **dns** 的時間)

**-o**：顯示活動的 **TCP** 連線並且包含每個連線程序的 **ID** 編號(**PID**)。你能夠找到應用程式的程序的 **PID** 資訊，在 **windows** 的工作管理員。這個參數通常和 **-a**, **-n**, and **-p** 混合使用。

**-p** 通訊協定：顯示指連線的通訊協定。預設的狀況這個通訊協定包含 **tcp**, **udp**, **tcpv6**, or **udpv6**。如果配合 **-s** 參數則是顯示統計數量。

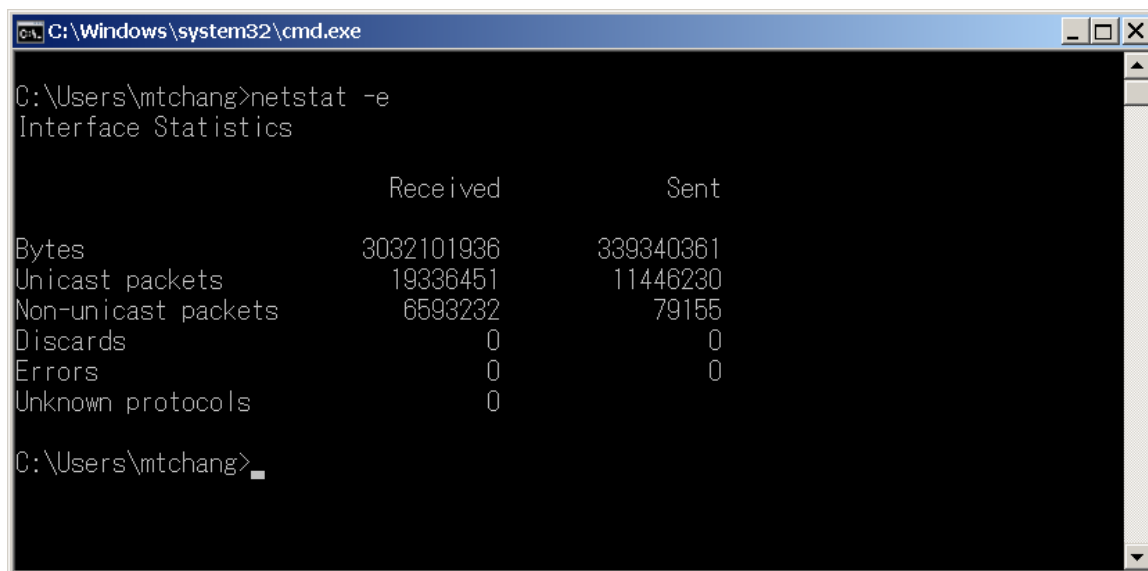
**-s**：顯示統計資訊。預設顯示 **TCP**, **UDP**, **ICMP**, and **IP** 通訊協定。如果 **IPv6 protocol for Windows XP** 被安裝的話，統計資料顯示 **TCP over IPv6**, **UDP over IPv6**, **ICMPv6**, and **IPv6 protocols**。

**-r**：顯示 **IP** 路由表的內容。相當於 **route print** 命令。

**Interval**：每隔幾秒重新顯示資訊。按 **CTRL+C** 可以停止顯示。如果省略則只顯示一次。

**/?**：此說明

**netstat -e** 顯示網路的統計資訊，如 **bytes** 數和封包發送和接收的數量



```
C:\Windows\system32\cmd.exe
C:\Users\mtchang>netstat -e
Interface Statistics

              Received              Sent
Bytes          3032101936          339340361
Unicast packets    19336451          11446230
Non-unicast packets  6593232           79155
Discards           0              0
Errors             0              0
Unknown protocols  0
C:\Users\mtchang>
```

**netstat -n** 顯示活動的 TCP 連線，但是 ip address 和 port 編號沒有被解釋翻譯成為名稱

```
C:\Windows\system32\cmd.exe
C:\Users\mtchang>netstat -n

Active Connections

Proto Local Address          Foreign Address         State
TCP    127.0.0.1:5354          127.0.0.1:57355        ESTABLISHED
TCP    127.0.0.1:5939          127.0.0.1:49181        ESTABLISHED
TCP    127.0.0.1:49164          127.0.0.1:49165        ESTABLISHED
TCP    127.0.0.1:49165          127.0.0.1:49164        ESTABLISHED
TCP    127.0.0.1:49179          127.0.0.1:49180        ESTABLISHED
TCP    127.0.0.1:49180          127.0.0.1:49179        ESTABLISHED
TCP    127.0.0.1:49181          127.0.0.1:5939         ESTABLISHED
TCP    127.0.0.1:49269          127.0.0.1:49270        ESTABLISHED
TCP    127.0.0.1:49270          127.0.0.1:49269        ESTABLISHED
TCP    127.0.0.1:49271          127.0.0.1:49272        ESTABLISHED
TCP    127.0.0.1:49272          127.0.0.1:49271        ESTABLISHED
TCP    127.0.0.1:57355          127.0.0.1:5354         ESTABLISHED
TCP    127.0.0.1:58442          127.0.0.1:58443        ESTABLISHED
TCP    127.0.0.1:58443          127.0.0.1:58442        ESTABLISHED
TCP    127.0.0.1:58444          127.0.0.1:58445        ESTABLISHED
TCP    127.0.0.1:58445          127.0.0.1:58444        ESTABLISHED
TCP    127.0.0.1:60535          127.0.0.1:60536        ESTABLISHED
TCP    127.0.0.1:60536          127.0.0.1:60535        ESTABLISHED
TCP    127.0.0.1:60537          127.0.0.1:60538        ESTABLISHED
TCP    127.0.0.1:60538          127.0.0.1:60537        ESTABLISHED
TCP    140.117.69.183:49152    140.117.69.203:3260    ESTABLISHED
```

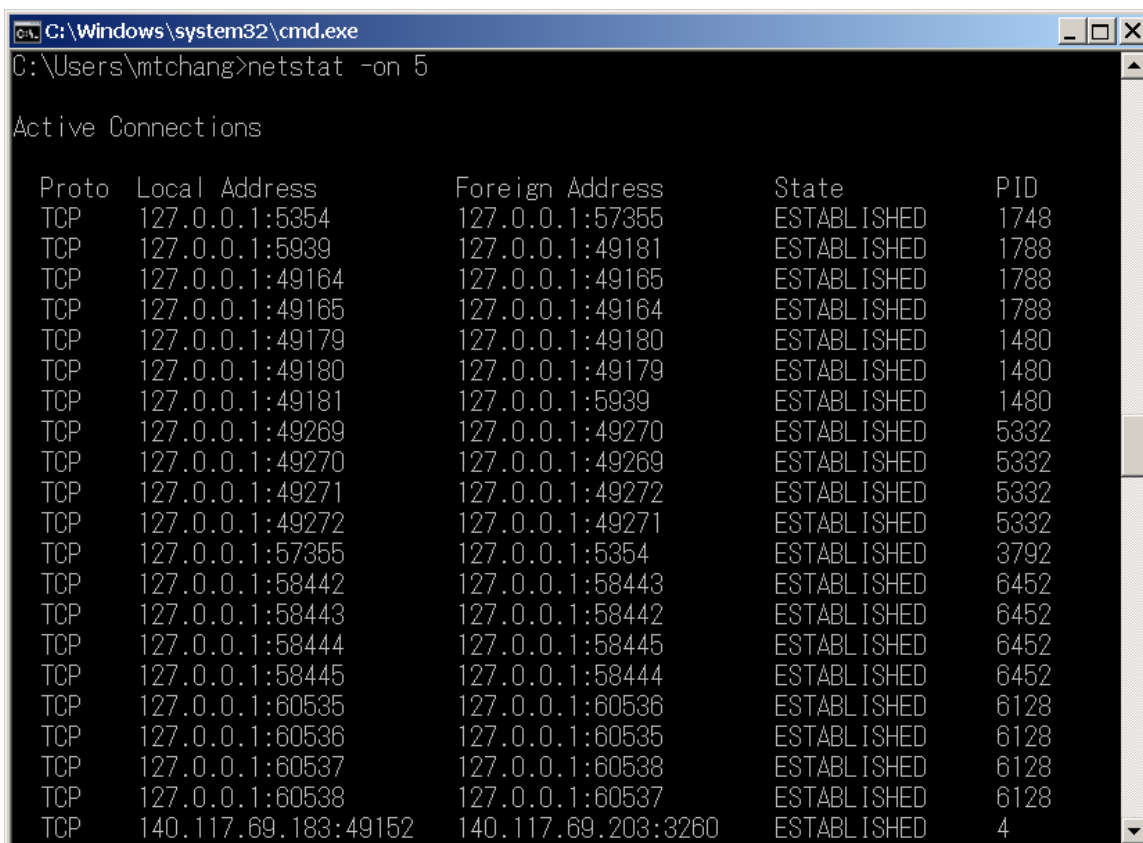
**netstat -o** 顯示活動的 TCP 連線並且包含每個連線程序的 ID 編號(PID)

```
C:\Windows\system32\cmd.exe
C:\Users\mtchang>netstat -o

Active Connections

Proto Local Address          Foreign Address         State      PID
TCP    127.0.0.1:5354          dbregistration:57355    ESTABLISHED 1748
TCP    127.0.0.1:5939          dbregistration:49181    ESTABLISHED 1788
TCP    127.0.0.1:49164          dbregistration:49165    ESTABLISHED 1788
TCP    127.0.0.1:49165          dbregistration:49164    ESTABLISHED 1788
TCP    127.0.0.1:49179          dbregistration:49180    ESTABLISHED 1480
TCP    127.0.0.1:49180          dbregistration:49179    ESTABLISHED 1480
TCP    127.0.0.1:49181          dbregistration:5939     ESTABLISHED 1480
TCP    127.0.0.1:49269          dbregistration:49270    ESTABLISHED 5332
TCP    127.0.0.1:49270          dbregistration:49269    ESTABLISHED 5332
TCP    127.0.0.1:49271          dbregistration:49272    ESTABLISHED 5332
TCP    127.0.0.1:49272          dbregistration:49271    ESTABLISHED 5332
TCP    127.0.0.1:57355          dbregistration:5354     ESTABLISHED 3792
TCP    127.0.0.1:58442          dbregistration:58443    ESTABLISHED 6452
TCP    127.0.0.1:58443          dbregistration:58442    ESTABLISHED 6452
TCP    127.0.0.1:58444          dbregistration:58445    ESTABLISHED 6452
TCP    127.0.0.1:58445          dbregistration:58444    ESTABLISHED 6452
TCP    127.0.0.1:60535          dbregistration:60536    ESTABLISHED 6128
TCP    127.0.0.1:60536          dbregistration:60535    ESTABLISHED 6128
TCP    127.0.0.1:60537          dbregistration:60538    ESTABLISHED 6128
TCP    127.0.0.1:60538          dbregistration:60537    ESTABLISHED 6128
TCP    140.117.69.183:49152    sc220369:3260          ESTABLISHED 4
```

**netstat -on 5** 顯示活動的 TCP 連線，不翻譯 DNS 名稱，每隔五秒顯示更新。



```
C:\Windows\system32\cmd.exe
C:\Users\mtchang>netstat -on 5

Active Connections

Proto Local Address          Foreign Address         State       PID
TCP   127.0.0.1:5354           127.0.0.1:57355        ESTABLISHED 1748
TCP   127.0.0.1:5939           127.0.0.1:49181        ESTABLISHED 1788
TCP   127.0.0.1:49164          127.0.0.1:49165        ESTABLISHED 1788
TCP   127.0.0.1:49165          127.0.0.1:49164        ESTABLISHED 1788
TCP   127.0.0.1:49179          127.0.0.1:49180        ESTABLISHED 1480
TCP   127.0.0.1:49180          127.0.0.1:49179        ESTABLISHED 1480
TCP   127.0.0.1:49181          127.0.0.1:5939         ESTABLISHED 1480
TCP   127.0.0.1:49269          127.0.0.1:49270        ESTABLISHED 5332
TCP   127.0.0.1:49270          127.0.0.1:49269        ESTABLISHED 5332
TCP   127.0.0.1:49271          127.0.0.1:49272        ESTABLISHED 5332
TCP   127.0.0.1:49272          127.0.0.1:49271        ESTABLISHED 5332
TCP   127.0.0.1:57355          127.0.0.1:5354         ESTABLISHED 3792
TCP   127.0.0.1:58442          127.0.0.1:58443        ESTABLISHED 6452
TCP   127.0.0.1:58443          127.0.0.1:58442        ESTABLISHED 6452
TCP   127.0.0.1:58444          127.0.0.1:58445        ESTABLISHED 6452
TCP   127.0.0.1:58445          127.0.0.1:58444        ESTABLISHED 6452
TCP   127.0.0.1:60535          127.0.0.1:60536        ESTABLISHED 6128
TCP   127.0.0.1:60536          127.0.0.1:60535        ESTABLISHED 6128
TCP   127.0.0.1:60537          127.0.0.1:60538        ESTABLISHED 6128
TCP   127.0.0.1:60538          127.0.0.1:60537        ESTABLISHED 6128
TCP   140.117.69.183:49152     140.117.69.203:3260    ESTABLISHED 4
```

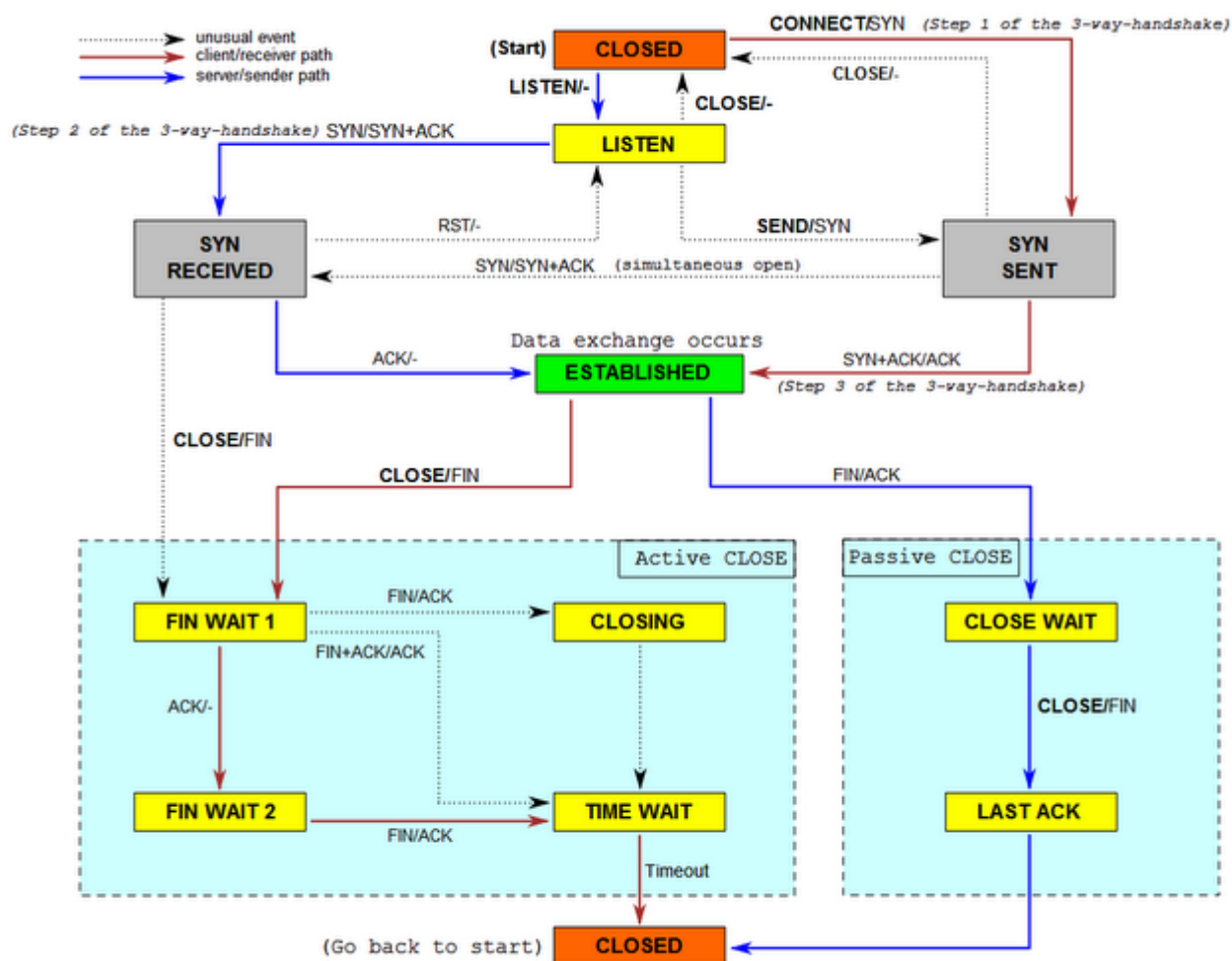
在這些資訊中，Proto 協定有兩個選項 TCP 及 UDP，Local Address 是指的是本地端的位置及 port 編號對應遠端的 Foreign Address 位置，State 則表示的此連線狀態狀況。通常我們對於 LISTEN 及 ESTABLISHED 的連線需要特別注意，因為那是和本台電腦有建立通訊連線服務。至於狀態有很多種不同的方式與型態，須要先瞭解關於 TCP 連線的的溝通方式。

## Protocol 的執行過程描述：

下圖描述為一張簡化的 TCP 狀態圖，更詳細的動作可以看 javed

&rzaghal(<http://www.medianet.kent.edu/techreports/TR2005-07-22-tcp-EFSM.pdf>) 寫的這篇。

以下引用自 [http://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](http://en.wikipedia.org/wiki/Transmission_Control_Protocol)



TCP 通訊過程可分為三個階段。且必須正確建立連接在一個很多步驟的交握處理(handshake process)然後才進入建立連接(connection establishment)，再進入資料傳輸(data transfer) 階段。資料傳輸完成後，最後連接終止(connection termination)建立的虛擬通道關閉並釋放所有分配的資源。

一個 TCP 連接是由作業系統所管理，TCP 連線基本上經歷底下這些變化：

1. LISTEN:如果是服務程式的話，指的是等待連接請求從任何遠端的客戶端。
2. SYN-SENT:等待遠端點對點發回一個 TCP segment 並帶有 SYN 和 ACK flag。通常做這件事的為 TCP 客戶端。
3. SYN-RECEIVED:等待遠端通道的另一端發回一個確認後發回確認連接到遠程節點。通常做這件事的為 TCP 服務端。
4. ESTABLISHED: port 準備好接收/及發送數據從到遠端節點。
5. FIN-WAIT-1 主動端發出 FIN 至被動端，並等待被動端回應 FIN 的 ACK
6. FIN-WAIT-2 成功接收到先前傳送至被動端 FIN 的 ACK，此刻等待被動端傳送 FIN
7. CLOSE-WAIT 被動端已接收主動端的 FIN，並傳送 FIN 的 ACK 至主動端，此刻等待 AP 要求關閉連線
8. CLOSING 進入 CLOSING 狀態雙方都同意關閉
9. LAST-ACK 先前收到主動端的 FIN，且傳送 FIN 的 ACK 給主動端，另被動端傳送 FIN 給主動端，此刻被動端等待主動端回應 FIN 的 ACK
10. TIME-WAIT:指等待足夠的時間，以確保通過遠端對等機器收到確認其連接終止請求。根據 RFC 793 中的連接可以

等到最久為四分鐘。

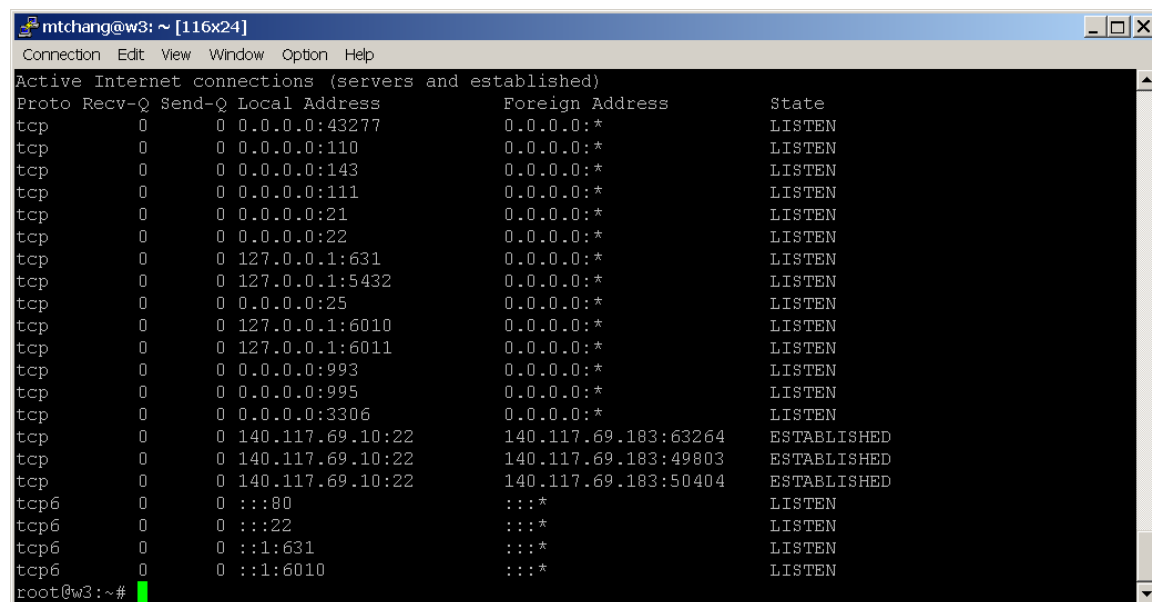
## 11. CLOSED 連線不存在於連線表

詳細網路協定可以參考：市面上的 [TCP/IP](#) 書籍

在 Linux 上也有一樣的指令，只是語法有點不同原理是一樣的。使用 `Linux man` 也可以拿到上面描述的文件。

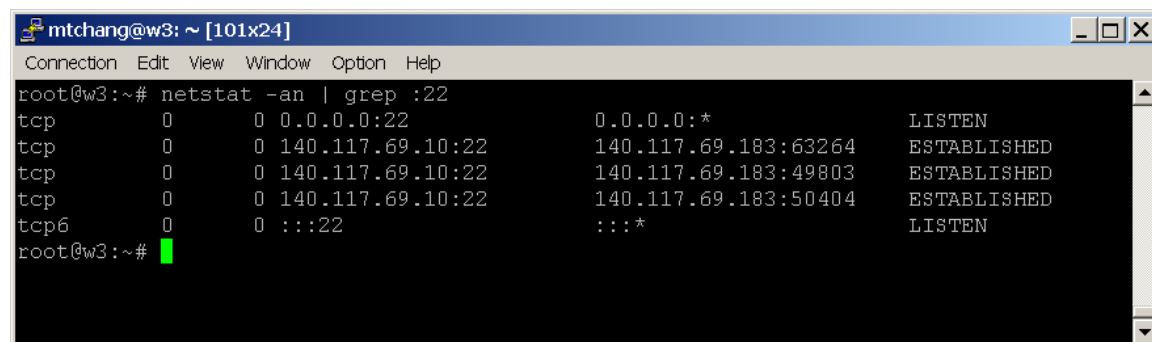
以下是一些實用的 `netstat` 語法，可以檢查主機的連線數量：

`netstat -na` 顯示主機上所有已建立的連線。



```
mtchang@w3: ~ [116x24]
Connection Edit View Window Option Help
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:43277          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:6010         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:6011         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:993            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306           0.0.0.0:*               LISTEN
tcp        0      0 140.117.69.10:22       140.117.69.183:63264    ESTABLISHED
tcp        0      0 140.117.69.10:22       140.117.69.183:49803    ESTABLISHED
tcp        0      0 140.117.69.10:22       140.117.69.183:50404    ESTABLISHED
tcp6       0      0 :::80                  :::*                     LISTEN
tcp6       0      0 :::22                  :::*                     LISTEN
tcp6       0      0 :::1:631                :::*                     LISTEN
tcp6       0      0 :::1:6010                :::*                     LISTEN
root@w3:~#
```

`netstat -an | grep :22` 顯示所有 port 22 的 sshd 的連線



```
mtchang@w3: ~ [101x24]
Connection Edit View Window Option Help
root@w3:~# netstat -an | grep :22
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN
tcp        0      0 140.117.69.10:22       140.117.69.183:63264    ESTABLISHED
tcp        0      0 140.117.69.10:22       140.117.69.183:49803    ESTABLISHED
tcp        0      0 140.117.69.10:22       140.117.69.183:50404    ESTABLISHED
tcp6       0      0 :::22                  :::*                     LISTEN
root@w3:~#
```

`netstat -alpn` 列出連線的協定及使用的應用程式，使用 IP 顯示

```
mtchang@w3: ~ [116x24]
Connection Edit View Window Option Help

root@w3:~# netstat -alpn | more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:43277           0.0.0.0:*               LISTEN      1188/rpc.statd
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      2721/pop3-login
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      9191/dovecot
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      1176/portmap
tcp        0      0 140.117.69.10:80        61.135.249.208:44947   SYN_RECV    -
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      19083/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      23992/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      1848/cupsd
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      12470/postgres
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      11086/master
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      3245/0
tcp        0      0 127.0.0.1:6011          0.0.0.0:*               LISTEN      10808/2
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      9191/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      2721/pop3-login
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      14458/mysqld
tcp        0    52 140.117.69.10:22        140.117.69.183:63264   ESTABLISHED 27473/sshd: mtchang
tcp        0      0 140.117.69.10:22        140.117.69.183:49803   ESTABLISHED 3238/sshd: mtchang
tcp        0      0 140.117.69.10:22        140.117.69.183:50404   ESTABLISHED 10803/sshd: mtchang
tcp6       0      0 :::80                   :::*                    LISTEN      10427/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      23992/sshd
tcp6       0      0 :::1:631                :::*                    LISTEN      1848/cupsd
```

以上是 Windows 及 Linux 的用法透過簡單的 netstat 指令可以用來判斷常見的系統及網路問題  
如果還是沒辦法解可以試試看在 windows 上的 TCPView v3.04 這個軟體，  
<http://technet.microsoft.com/en-us/sysinternals/bb897437>  
TCPView 是一個 Windows 程序，它會顯示所有 TCP 和 UDP 服務的狀態，包括本地和遠端位址和狀態的 TCP 連接狀態。  
還可以觀測每個程序所發送的流量狀態 是個用來取代 netstat 的好用工具。

TCPView - Sysinternals: www.sysinternals.com										
File Options Process View Help										
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Recv Pack
chrome.exe	5988	TCP	mtchang-win7	62331	ht-in-f189.1e100.net	https	ESTABLISHED	8	15,872	
chrome.exe	5988	TCP	mtchang-win7	61763	ht-in-f189.1e100.net	https	ESTABLISHED	7	13,881	
WINWORD.EXE	2796	TCP	mtchang-win7	63986	ht-in-f100.1e100.net	https	ESTABLISHED	14	10,895	
chrome.exe	5988	TCP	mtchang-win7	63752	channel2-02-07-sncf.facebook.com	http	ESTABLISHED	8	8,795	
chrome.exe	5988	TCP	mtchang-win7	64045	tt-in-f104.1e100.net	http	ESTABLISHED	5	7,137	
chrome.exe	5988	TCP	mtchang-win7	62279	ht-in-f83.1e100.net	https	ESTABLISHED	5	6,617	
chrome.exe	5988	TCP	mtchang-win7	63706	www-10-05-pm1.facebook.com	http	ESTABLISHED	8	5,996	
chrome.exe	5988	TCP	mtchang-win7	64085	tt-in-f104.1e100.net	http	ESTABLISHED	4	5,865	
chrome.exe	5988	TCP	mtchang-win7	64057	tt-in-f102.1e100.net	http	ESTABLISHED	4	5,034	
firefox.exe	5332	TCP	mtchang-win7	64035	tt-in-f19.1e100.net	https	ESTABLISHED	2	4,911	
chrome.exe	5988	TCP	mtchang-win7	64084	tt-in-f104.1e100.net	http	ESTABLISHED	3	4,395	
chrome.exe	5988	TCP	mtchang-win7	59643	ht-in-f17.1e100.net	https	ESTABLISHED	2	4,123	
System	4	UDP	mtchang-win7	netbios-ns	*	*		60	3,000	
firefox.exe	5332	TCP	mtchang-win7	64102	tt-in-f19.1e100.net	https	ESTABLISHED	2	2,988	
chrome.exe	5988	TCP	mtchang-win7	64066	tt-in-f102.1e100.net	http	ESTABLISHED	2	2,964	
chrome.exe	5988	TCP	mtchang-win7	64083	tt-in-f104.1e100.net	http	ESTABLISHED	2	2,951	
firefox.exe	5332	TCP	mtchang-win7	64104	tt-in-f189.1e100.net	https	ESTABLISHED	2	2,901	
chrome.exe	5988	TCP	mtchang-win7	63991	tt-in-f113.1e100.net	http	ESTABLISHED	3	2,875	
chrome.exe	5988	TCP	mtchang-win7	64099	140.117.13.108	http	ESTABLISHED	6	2,673	
chrome.exe	5988	TCP	mtchang-win7	64038	ht-in-f100.1e100.net	https	ESTABLISHED	2	2,622	
instantbird.exe	6452	TCP	mtchang-win7	64105	baymsgl1010804.gateway.edge.messenge... msnp		ESTABLISHED	4	1,876	
chrome.exe	5988	TCP	mtchang-win7	64061	iy-in-f101.1e100.net	http	ESTABLISHED	3	1,599	
chrome.exe	5988	TCP	mtchang-win7	64087	tt-in-f104.1e100.net	http	ESTABLISHED	1	1,466	
chrome.exe	5988	TCP	mtchang-win7	64086	tt-in-f104.1e100.net	http	ESTABLISHED	1	1,465	
chrome.exe	5988	TCP	mtchang-win7	64088	a60-254-140-160.deploy.akamaitechnolo... http		ESTABLISHED	1	1,390	
[System Process]	0	TCP	mtchang-win7	64013	a60-254-140-162.deploy.akamaitechnolo... http		TIME_WAIT	1	1,265	
chrome.exe	5988	TCP	mtchang-win7	64047	tt-in-f106.1e100.net	http	ESTABLISHED	1	1,076	
instantbird.exe	6452	TCP	mtchang-win7	64103	baymsgl1010805.gateway.edge.messenge... msnp		ESTABLISHED	3	1,025	

Endpoints: 221 | Established: 79 | Listening: 33 | Time Wait: 14 | Close Wait: 7