網路連線狀態

使用者收到中心通知的異常網路行為信件後，通常的處理方式不是掃毒就是重灌電腦。但是有部分使用者會來電詢問，要如何得知自己電腦執行中的程式的網路連線資訊。下列介紹幾個工具，可以讓使用者檢測目前電腦中哪些軟體開啟了哪些網路連線，藉此對自己的電腦軟體網路使用行為有更完整的了解。

常用指令

netstat - windows

netstat - linux

視窗軟體

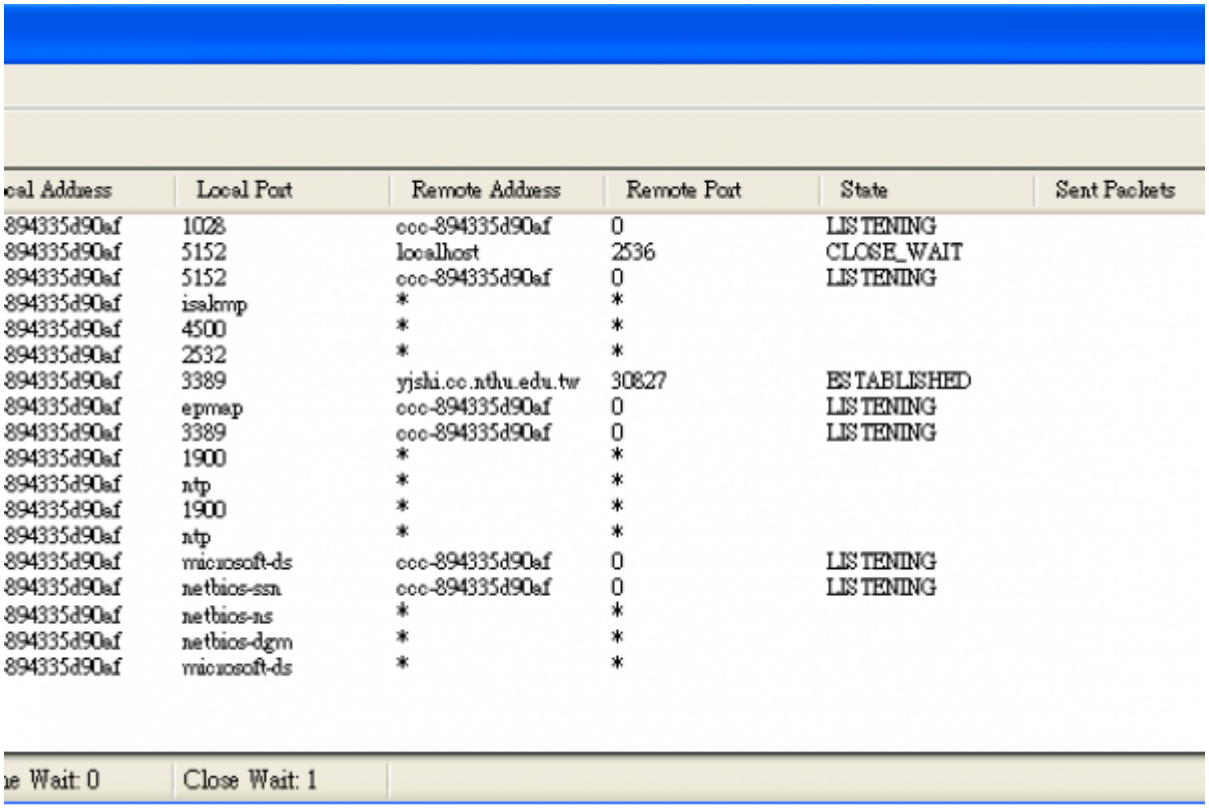
Symantec Endpoint Protection

學校簽訂的安全防護軟體Symantec Endpoint Protection中，就有提供相關功能來檢視電腦上執行及存取網路的應用程式和服務。

Windows Sysinternals TCPview

TCPview可以顯示Windows作業系統上，所有TCP與UDP網路連接埠的詳細清單，內容包含本地與遠端的位址及TCP連線的狀態。在Windows Server 2008、Vista與XP及後續的OS版本中，TCPView還可以顯示使用連接埠的程式名稱。

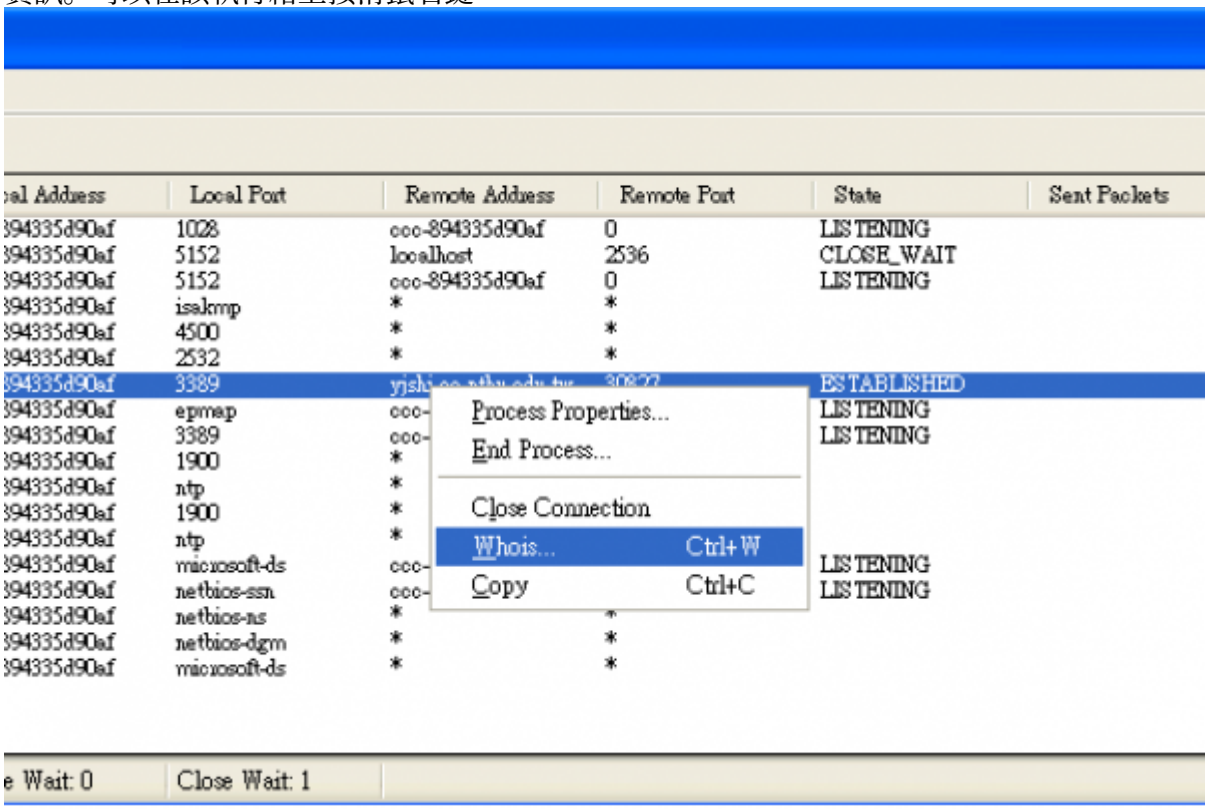
當我們執行TCPview



Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets
894335d90af	1028	ccc-894335d90af	0	LISTENING	
894335d90af	5152	localhost	2536	CLOSE_WAIT	
894335d90af	5152	ccc-894335d90af	0	LISTENING	
894335d90af	isakmp	*	*		
894335d90af	4500	*	*		
894335d90af	2532	*	*		
894335d90af	3389	yjshi.cc.nthu.edu.tw	30827	ESTABLISHED	
894335d90af	epmap	ccc-894335d90af	0	LISTENING	
894335d90af	3389	ccc-894335d90af	0	LISTENING	
894335d90af	1900	*	*		
894335d90af	ntp	*	*		
894335d90af	1900	*	*		
894335d90af	ntp	*	*		
894335d90af	microsoft-ds	ccc-894335d90af	0	LISTENING	
894335d90af	netbios-ssn	ccc-894335d90af	0	LISTENING	
894335d90af	netbios-ns	*	*		
894335d90af	netbios-dgm	*	*		
894335d90af	microsoft-ds	*	*		

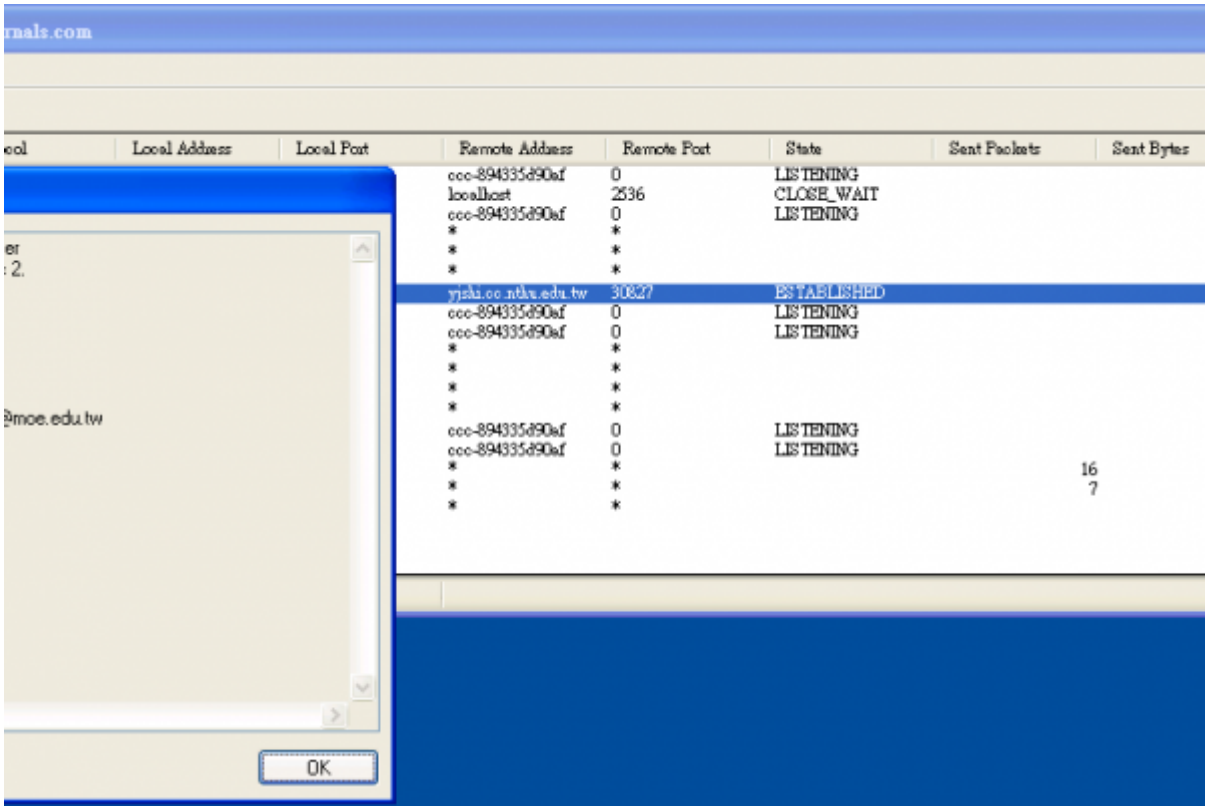
e Wait: 0 Close Wait: 1

可以看到目前電腦執行中有開啟連線埠的所有執行緒。當我們對某支執行緒對外連線的IP想要有更詳細的資訊。可以在該執行緒上按滑鼠右鍵



e Wait: 0 Close Wait: 1

選擇WHOIS即可列出該IP的所在國家、使用單位、管理人員等資料。



TCPview 詳細資訊
下載 TCPview

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/security:netstat

Last update: **2013/05/09 09:38**