

快速連結

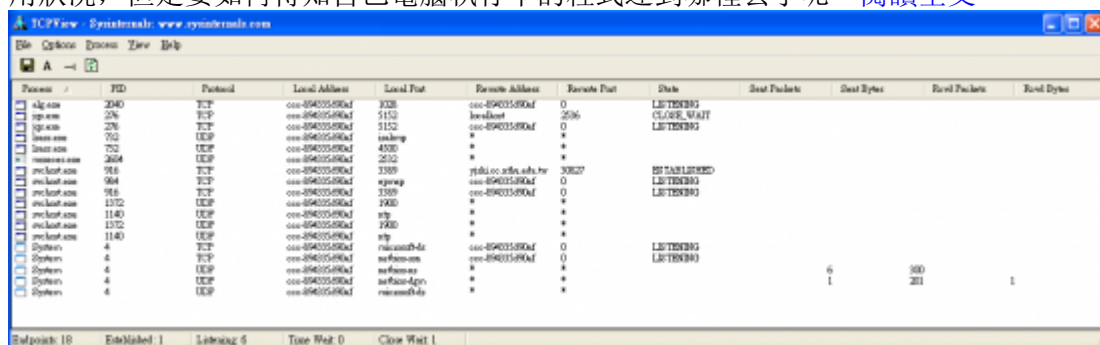
- [本組最新消息](#)
- [資通安全](#)
- [聯絡我們](#)

[收到此電子報是因為您是本組的服務對象，詳情請參閱發行說明](#)

2013.05 第二十四期：您知道您的電腦連到哪裡去了嗎？

您知道您的電腦連到哪裡去了嗎？

最近中心發現多起電腦疑似遭入侵植入木馬或成為Botnet一員的殭屍電腦事件，使用者收到中心通知異常網路行為的信件後，通常的處理方式不是掃毒就是重灌電腦。部分使用者想要更進一步了解電腦的網路使用狀況，但是要如何得知自己電腦執行中的程式連到哪裡去了呢…[閱讀全文](#)



The screenshot shows the TCPView application window with a list of active network connections. The columns include Process, PID, Protocol, Local Address, Local Port, Remote Address, Remote Port, State, Sent Packets, Sent Bytes, Received Packets, and Received Bytes. Several connections are visible, including those to localhost and various external IP addresses.

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Received Packets	Received Bytes
alg.exe	2040	TCP	000-094035-0000	8080	000-094035-0000	0	LISTENING				
alg.exe	2040	TCP	000-094035-0000	8080	localhost	2536	ESTABLISHED				
alg.exe	2040	TCP	000-094035-0000	8080	localhost	0	LISTENING				
alg.exe	752	UDP	000-094035-0000	4300	*	*	*				
alg.exe	752	UDP	000-094035-0000	4300	*	*	*				
alg.exe	2648	UDP	000-094035-0000	2536	*	*	*				
alg.exe	916	TCP	000-094035-0000	3389	192.168.1.100:3389	3389	ESTABLISHED				
alg.exe	916	TCP	000-094035-0000	3389	localhost	0	LISTENING				
alg.exe	1372	UDP	000-094035-0000	1900	*	*	*				
alg.exe	1140	UDP	000-094035-0000	1900	*	*	*				
alg.exe	1372	UDP	000-094035-0000	1900	*	*	*				
alg.exe	1140	UDP	000-094035-0000	1900	*	*	*				
System	4	TCP	000-094035-0000	1900	localhost	0	LISTENING				
System	4	TCP	000-094035-0000	1900	localhost	0	LISTENING				
System	4	UDP	000-094035-0000	1900	*	*	*				
System	4	UDP	000-094035-0000	1900	*	*	*				

訊息快報

本校分機免費撥打中華電信、遠傳及台灣大哥大等電信業者之MVPN群組行動電話

本校分機即日起可免費撥打已加入本校之中華電信、遠傳及台灣大哥大等電信業者之MVPN群組行動電話，歡迎全校師生自行申請加入。加入清大MVPN行動電話群組方式、撥打方式…[閱讀全文](#)

資安宣導

1. 注意電子郵件詐騙

2013年04月13日（六）有用戶收到詐騙信主旨為「帳戶維護計劃」，詐騙信內文如下所示 (The following example is a phishing scam. Delete it once you receive it.)…[閱讀全文](#)

2. 注意 Open DNS resolver 問題

請各系所單位 DNS 管理者妥善管理伺服器，避免成為 Open DNS resolver 而遭校外 IP 利用發動 DDoS 網

路攻擊…[閱讀全文](#)

3. 個人電腦建議安裝步驟

在防火牆軟體尚未完成安裝前，就將電腦連接上網際網路，即是將充滿漏洞的系統暴露於網際網路中。此時，系統可能在安裝的過程中，就已經遭受到網路病毒的感染或是駭客的入侵攻擊。因此，個人電腦作業系統依建議的程序進行安裝，可避免在過程中遭受網路攻擊與病毒感染…[閱讀全文](#)

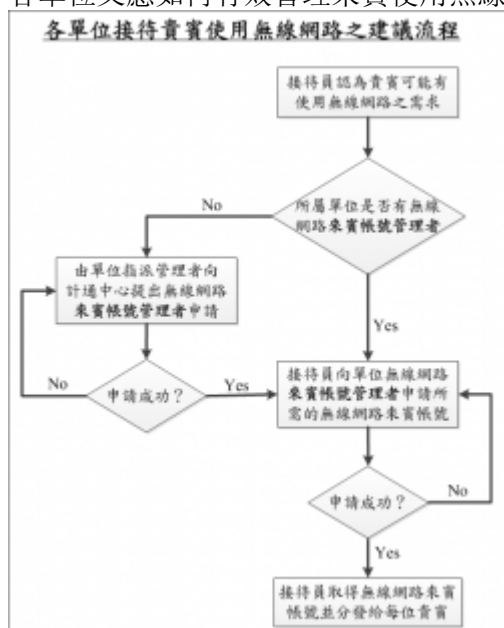
服務介紹

1. 服務狀態即時檢測

為讓使用者快速掌握網路系統組提供的各項服務伺服器是否正常，中心自99年已研發建置「服務狀態即時檢測」系統，整合各伺服器即時之服務狀態，提供使用者透過瀏覽器查詢服務現況，便於判別是否為伺服器端(Server)或是客戶端(Client)的問題。現階段已提供電子報系統□TWAREN SSL-VPN□Mail□Proxy□DNS□無線網路及校園網路等服務狀態資訊…[閱讀全文](#)

2. 無線網路來賓帳號管理

近年來學術交流頻繁，產學合作日趨密切，各單位無跨校漫遊帳號之來賓，應如何使用校園無線網路？而各單位又應如何有效管理來賓使用無線網路的狀況？基於以上考量，本中心建議…[閱讀全文](#)



網管技術專題

伺服器安全防護

為有效管理伺服器，減少系統因軟體漏洞或遭受外部攻擊造成損失，以下介紹各種系統安全設定方式及步驟，提供伺服器管理者參考，本範例以 CentOS 為例。其管理方式大致可分為以下三個階段…[閱讀全文](#)

好康資訊

雲端虛擬主機服務

為提昇本校電腦資源應用效益、降低各單位建置及維運成本，同時落實節能減碳政策，歡迎有**建置伺服器**、**需安全的網路防禦**或**個人行動辦公室**等需求之系所單位、實驗室教職員工多多利用，共創水木清華低碳校園。**即日起前60名新舊用戶方享有「第一年付費，第二年免費」優惠**，第三年恢復原價。**目前不包含本中心申請使用**，已有46名用戶，剩餘14名數量有限敬請把握...[閱讀全文](#)



發行說明：

電子報內容包含校園網路、網際網路應用、資通安全、校園電話等服務說明與各項公告，以及相關領域的專題報導。本刊物以網路系統組服務用戶為發行對象，訂閱者可收到定期電子報及不定期公告，建議您長期訂閱以獲得最新資訊。

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/mailling:201304_24

Last update: **2013/05/30 14:13**

