

圖一 國立故宮博物院無線網路建置架構圖

何時間、任何地點，針對個人的需求來取得最適當的服務，這已經逐漸成為我們生活環境的一部份。一條綁住行動的網路線，已經被科技的洪流所

# 一條看不見的線 · 連接全世界 故宮UNS網路建設與應用研製

施尚文

您記得，有多久沒來故宮了呢？

翠玉白菜依舊翠綠，毛公鼎上的銘文依舊迷人，清明上河圖中的人物仍是栩栩如生。您第一眼驚艷的或許是光鮮亮麗的展示空間，以及完善的導覽品質，但在這些有形的軟硬體設施之外，還有您看不見卻隨時隨地隨手可得的服務——國立故宮博物院（NSM）網路建設帶來的科技便利性。

「縱橫五千年·悠遊掌中天」是我們新世紀U化故宮優質園區示

範計畫的口號，期望透過建置本院U化基礎建設等資訊技術來達成。一年前這是口號、是目標、是期望；現在，這是事實，已經建置完成，並存在於院區之中。雖然看不見也摸不著，可是它確實全部建置完成，並且已經默默地提供服務。

故宮向來以保存、展示、研究、教育等各領域來提供社會對華夏文物的認識，為了做到最完善的服務，借用網路科技的力量是必需的。早先，

沖斷，目前無線網路的普及性，讓使用者可隨時隨地取得資訊。

建置U化故宮無線網路基礎建設，無論對參訪者，還是故宮的內部工作人員，都是給予跨越新世代獲得資訊的利器。對使用者而言，全院無線網路服務所帶來的衝擊是當需要資訊時，不再是尋找硬體位置，而是尋找即時大量資訊的方法，您不用煩惱該至何處上網查詢，您只須關心隨手可得的資訊會不會太多。

## U化故宮無線網路基礎建設

「U化故宮無線網路基礎建設」的主要目標為以建置故宮全院無線網路基礎建設，提供優質網路與發展環境，進而配合推展U化故宮數位博物館網站、即時的U化博物館服務資訊、建置文物PDA、及文物展覽或庫房管理等計畫，最終達成「國家資訊通信發展方案」之發展優質網路社會的策略目標。

無線網路的方便，讓人們可以隨時隨地上網，但卻造成許多安全管理上的問題；例如因為資訊容易取得，

我們以網路基礎建設為U化工程中最重要的一環，要求安全、穩定、快速的網路，因此建置故宮聯外寬頻網路，用以提供U化博物館資訊服務與大眾分享。提升U化故宮網路的服務品質與速度，亦提升了故宮博物院在世界博物館界的競爭能力。

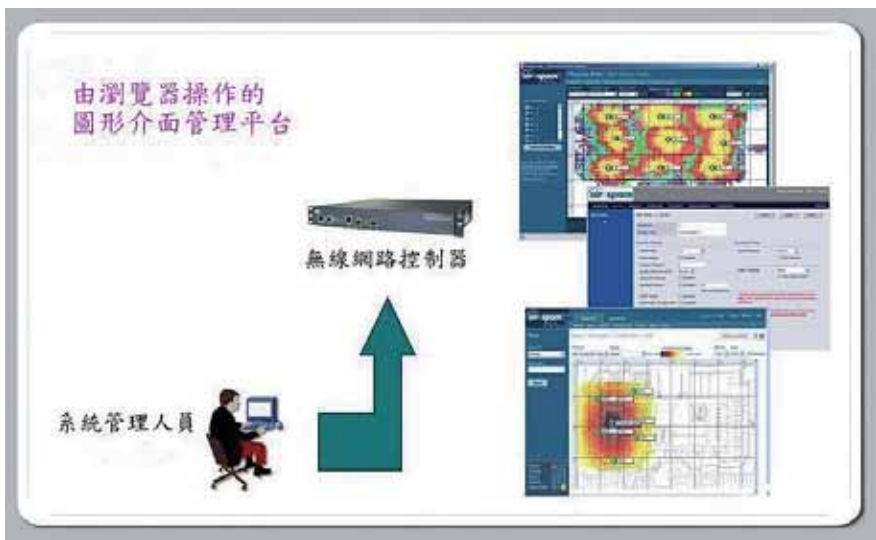
## U化故宮全院無線網路服務

人們對於網路的需求，從固定於電腦硬體前，到現在隨身裝置，在任

有心人士可在沒有管理的情況下，利用無線網路破壞系統、盜取帳號等違法行為，因此無線網路安全管理機制的建立，為本計畫重要的考量，建置以「分散架構」、「集中管理」的無線網路認證管理系統。藉由無線控管交換器控制建築物內的無線基地台接續點（Access Point, AP），及無線網路的接取，結合後端認證管理系統整合，提供使用者一個安全又便利的無線網路環境。

無線網路認證管理系統需有效授權使用者存取網路，還需能夠監測各接續點之連線運作是否正常，同時得線上即時監控、管理、紀錄無線網路上各使用者的使用情況。使用者在操作無線網路時，不必更動電腦的設定，也不必額外安裝任何軟體。換句話來說，就是要在不需改變使用者及管理人員的設備與使用習慣，且不犧牲網路的安全架構及管理方式下，完成無線網路的建置，並提供跨網段的漫遊服務（如圖二）。

## 建置無線網路規劃內容



圖三 國立故宮博物院無線網路設備管理平台

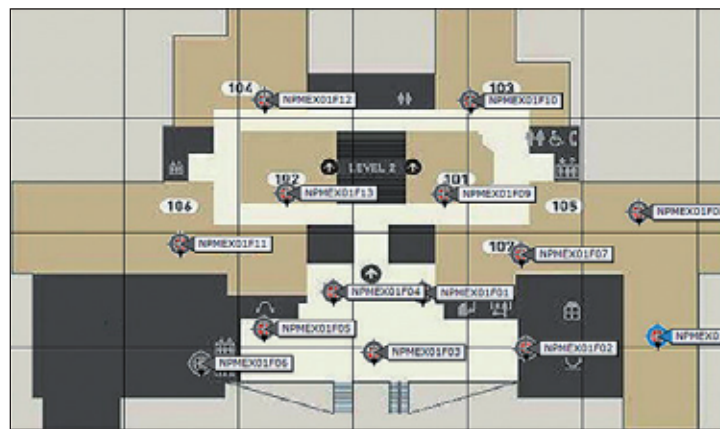
系統管理人員  
無線網路控制器

由瀏覽器操作的  
圖形介面管理平台

個帳號訂定不同的使用時間，  
使存取網路資源更暢順。

(三) 無線網路設備均支援無縫漫遊

無線基地台使用無線網路供電  
(Power over Ethernet: PoE) 功能，因無  
線基地台大多隱藏於天花板或牆壁  
上，這些位置大多不具備電源插座，



圖四 國立故宮博物院正館展廳101室至107室無線網路基地台配置圖

功能，可讓使用者遊走於不  
同虛擬區網分段 (Virtual Local  
Area Network: VLAN)，或是跨  
越不同的網域時無需重新登  
入，並可滿足支援語音流量，  
且所有的控制器應用設備會共  
用使用者資訊和授權。

對於所提出的無線網路系統，利  
用思科無線網路控制器 (Cisco WLAN  
Controller)，搭配輕級無線網路存取協  
定 (Light Weight Access Point Protocol:  
LWAPP) 1131AAG 的接續點做為無線存  
取設備的架構，而這些設備利用無線  
網路控制系統 (Wireless Control System;  
WCS) 統一安全管理。驗證及帳號管  
理部份採用思科帳號權限管理伺服器  
(Access Control Server: Cisco ACS) 作為  
管理平台。

也不可能特地設電源線，因此無線基  
地台具有無線網路供電功能，只要具  
備 10/100BASE-T 即可，不用額外佈署  
電源線，建置方式也較容易，機櫃端  
數量超過三點則提供供電交換器，用  
以收攏大量的無線基地台，如此較具  
彈性。



圖二 國立故宮博物院正館展廳室內無線網路基地台

無線網路之功能建置

(一) 於無線網路控制器上建置多  
個服務組識別碼 (Service Set  
Identifier: SSID)，如 LAN1、  
LAN2 等，開放給特別來賓部  
份，採線上驗證方式並將瀏覽  
器強制導至故宮首頁；院內員  
工部份，則啟用 802.1X 及 MAC  
驗證，並可依院內需求設置更  
多服務組識別碼。

(二) 配合遠端用撥入驗證服務伺服  
器 (Remote Authentication Dial

器) 提供  
強資訊安全考量，使用者認證與加密  
必須強固，以防止非院內員工使用非  
院內電腦存取院內之網路，造成資訊  
安全問題。因此運用了業界最嚴格  
的安全管理 802.1X 認證機制配合院內  
有員工之帳號認證，以加強資訊安  
全。

(三) 「特別來賓」使用無線網路  
此區域無線網路的運用，在於提  
供特定的或特別來賓於演講廳、會議  
室等特定空間，有有限的上網。並與  
院內網路隔離，以防有心駭客的攻  
擊。

依使用者性質不同分為三類

(一) 「文物導覽、庫房管理」等應  
用

未來院內將提供無線導覽服務，  
以具無線功能之手持式設備為載具，

提供民眾透過無線網路存取導覽內容  
(多媒體或單純語音)，提高民眾看  
展的品質與深度。

(二) 「院內員工」使用無線網路  
此區域的無線網路運用，特別加



圖六 國立故宮博物院全院無線網路所涵蓋辦公區

能，一般通過院內申請認證的使用者，則授與院內資源存取及連線上網等服務，而且亦支援802.11x認證功能，有效強化認證安全。

兼顧認證、偵測等安全管理機制  
思科無線控制器具有偵測與阻擋

提供優質網路與發展環境，進而配合推廣U化故宮數位博物館網站、即時U化博物館服務資訊，並透過U化的高科技技術，達成鮮活呈現故

非法接續點與使用者功能，已為無線網路安全增添第一道防線，另外分割虛擬區網分段隔離有線網路，更能確保無線網路不會成為駭客入侵的漏洞。使用者認證方面，並採用安全套接層 (Secure Sockets Layer: SSL) 協定配合網頁介面讓使用者登入，除便於登入外，更能統一管理。

**成果效益**

本計畫推展無線網路至全院，包括正館、行政大樓、圖書文獻大樓、第二辦公大樓、保存維護處大樓及三處庫房等，總共建置無線基地台一二一顆，讓全院大部分涵蓋在無線網路訊號之下，加上前述之使用者認證、加密等安全機制，造就一個既快速又安全的網路環境，使得資訊的獲得成為隨手可得，這就是U化的精神。

參考資料

- 友訊科技股份有限公司 (2005)，無線區域網路技術白皮書。台北：文魁資訊。
- 國眾電腦股份有限公司 (2008)，「U化故宮無線網路基礎建置案」建議書。台北：國眾電腦股份有限公司。

作者任職於本院教育展覽處



圖五 國立故宮博物院正館室外無線網路基地台天線

無線基地台使用內建基本天線，基地台已內建支援使用802.11a及802.11b/g標準，管理者可依使用需

求，進行天線功能啟動調整；同時內建式天線亦免除外接天線所需的相關安裝及建置工程。

基地台使用輕級無線網路存取協定，基地台單點並不提供控制端 (Console) 之連接，所有參數設定由中心端無線控制器統一進行管控，對企圖竊取設備的有心人士而言，基地台在沒有控制器的前提下，也僅只是擴充式的天線，無法正常運作；且無控制端的連接，以避免於基地台架設地點，發生設定遭到修改等問題產生。

部署干擾小的無線網路環境

建置採用2.4GHz頻道，部署一、六、十一屬於獨立的頻道，避免干擾源，同時經由中心端無線控制器，動態地區分各頻道，以減少基地台間相互干擾的問題。

無線網路建置安全解析

院內安全的無線網路環境，考量的不僅是覆蓋率、頻寬等的使用性問題，重要的是如非法無線基地台、使用者、無線溢波，或是否受到其他無線基地台的干擾，會不會成為駭客入侵的大門等無線網路環境。

偵測警示非法訊號，捍衛無線安全

達到無線網路安全除偵測之外，更必須要能夠阻擋非法無線訊號，本案所採用的設備均能主動阻擋。採用思科無線網路控制器搭配專用輕級接續點 (light weight AP)，能偵測與阻擋非法訊號，除切割虛擬區網分段與有線網路隔離外，另具備無線網路控制系統的管理軟體監控無線訊號流量，即時以警訊方式通知管理者判別處理。

整合式內建帳號管理系統

考量統一管理帳號與使用者登入的方便性，提供內建式帳號管理系統，除方便使用者登入外，更能以設定多重加密的方式，強化認證安全，並同時增加漫遊功能（所有接續點上連接的使用者無論終端移動到哪個接續點下，使用者資訊和授權都在無線控制器所管轄的移動網域內快速交換，以實現無縫漫遊）。無線網路透過認證與授權的結合，當使用者登入無線網路服務後，依照使用者身份帳號的不同，提供不同的存取政策定義，特定的使用者具備連線及管理功

宮華夏文物之美的最重要目標，是我們的期望。

藉由無線網路環境，提供手持設備具有故宮內部分機通話功能，以及活動訊息、展覽資訊、故宮全院地圖導覽、訊息佈告、櫃門開啟資訊等功能，現已由正館展廳管理員使用。便利管理員即時獲得最需要的展覽活動資訊、活動說明，使觀眾獲得更親切具體的服務，有效提升服務品質。

此外，故宮文物保存環境溫溼度感知監測系統，也正由本院保存維護單位逐步建置中，結合無線網路，利用溫濕度感測器、資料收集器、網路伺服器等設備，發展出遠距無線監測，提供本院保存維護人員隨時監看文物典藏環境。