

# 建置中小學優質化均等數位教育環境計畫

## 無線網路建置實驗計畫



# 大綱

- 實驗測試結果。
- 無線網路資安問題。
- 各家廠商佈建成本比較。



# 實驗測試結果

## 無線網路認證及漫遊測試

	本市帳號認證	漫遊帳號認證
Aruba	●	●
Cisco AP	●	●
D-Link Thin AP	●	●
D-Link Fat AP	●	●
FON AP	●	●



# 實驗測試結果

## 電磁波強度測試

	Aruba	Cisco	D-Link Thin	D-Link Fat	FON
毫高斯	12.2	11.2	2.9	13	3.0

## Wi-Fi Phone跨 AP做漫遊

	Aruba	Cisco	D-Link Thin	D-Link Fat	FON
結果	●	●	●	●	●



# 實驗測試結果

## AP佈建方式與無線訊號

3F教室							
3F走廊		★				★	
2F屋內							
2F走廊	★			★			★
1F教室							
1F走廊		★				★	

●一般來說，平均三到四間教室佈建一台AP。建議將AP設置在走廊，訊號穿透力較好。

●AP供電方式，可採用POE Injector或POE Switch。



# 實驗測試結果

## 各種認證方式測試

	Aruba	Cisco	D-Link Thin	D-Link Fat	FON
WEB認證	●	●	●	●	●
MAC驗證	●	●	●	●	●
WPA2-PSK	●	●	●	●	●
WPA2	●	●	●	●	未測完成

★ D-Link Thin AP在進行 WEB認證時，所需時間超過15秒以上。



# 實驗測試結果

## SSID與認證規劃

	Aruba	Cisco	D-Link Thin	D-Link Fat	FON
SSID 1	WEB認證 MAC認證	WEB認證	WEB認證	WEB認證 MAC認證	WEB認證 MAC認證
SSID 2	WPA	MAC認證	MAC認證	WEB認證 WPA認證	WPA
SSID 3		WPA	WPA		



# 實驗測試結果

## 在NAT環境下進行測試

	Aruba	Cisco	D-Link	FON
IP分享器	●	●	無此功能	尚未測試
UNIX NAT (BrazilFW)	●	●	無此功能	尚未測試
廠牌Firewall (Sonicwall)	●	尚未測試	無此功能	尚未測試





# 實驗測試結果

## 流量在本地交換測試

	Aruba	Cisco	D-Link	FON
使用Public IP	●	●	無此功能	尚未測試
IP分享器之NAT	●	●	無此功能	尚未測試
UNIX NAT (BrazilFW)	●	●	無此功能	尚未測試
廠牌Firewall (Sonicwall)	●	尚未測試	無此功能	尚未測試



# 實驗測試結果

## Controller(Gateway)相關功能

	Aruba	Cisco	D-Link Thin	D-Link Fat	FON
分層管理	▲	▲	▲	●	● (需另購軟體)
訪客系統	▲	▲	無此功能	●	無此功能
NAT	●	無此功能	無此功能	●	無此功能
DHCP	▲	▲	▲	●	▲



# 無線網路資安問題

- Eavesdropping (竊聽)：
  - 攻擊方式：針對通訊內容進行監控或透過網路監聽，針對網路通訊流量、內容進行分析。
  - 因應對策：利用WPA2增強式加密技術，即使通訊內容被監聽，也不能被破解，保證了無線網路上傳輸資料的安全。
- Traffic Analysis (流量分析)：
  - 攻擊方式：針對網路通訊的流量、內容及行為進行分析，以獲得目標網路的資料。
  - 因應對策：對沒有加密或者使用弱加密技術加密的無線網路，通訊的內容是很容易被監聽。而使用WPA2/AES加密技術後，可為無線網路提供足夠的安全保障。



# 無線網路資安問題

- Masquerade (偽裝):
  - 攻擊方式：欺騙認證系統，非法取得系統資源最常見的有密碼盜用。
  - 因應對策：使用802.11i，即802.1X/EAP+AES-CCMP認證加密技術。必須經過授權認證的用戶才可使用網路，可有效的保證傳統WEP加密方式下密碼容易被破解的問題。
- Replay (重播):
  - 攻擊方式：透過網路截取的某些通訊內容再動新發送，最常見的莫過於重新發送認證資料。
  - 因應對策：透過802.1x的通訊協定. 可以將沒有通過的使用者將無法進入網路, 使其無法利用任何網路資源。某些廠商可以針對不規則的封包序號去做判斷，以識別該封包是否重複。



# 無線網路資安問題

- Message modification (訊息竄改)：
  - 攻擊方式：竄改無線網路通訊內容，傷害資料的完整性。
  - 因應對策：資料的完整性檢查，可以利用WPA2來解決。通過對使用者無線傳輸的資料包進行MIC編碼，確保使用者資料不被其他使用者更改。
- Session Hijacking (通訊劫奪)：
  - 攻擊方式：利用網路通訊弱點搶奪合作使用者的通訊頻道。
  - 因應對策：使用WPA2加密可降低此一攻擊的危險性。
- Denial-Of-Services (阻斷服務)：
  - 攻擊方式：針對系統進行攻擊，藉此使系統無法提供服務。
  - 因應對策：有些廠商提供此攻擊的偵測，除了發出告警訊息給管理者之外，並將攻擊者放入黑名單中。



# 無線網路資安問題

- Main-in-the-Middle (中間攻擊):
  - 攻擊方式：以較強的AP蓋過原有AP訊號，強迫用戶的無線網卡跳至攻擊者的AP，而用戶會以為是漫遊至另一個AP，並持續送出資料，進而截取到部份傳輸資料。
  - 因應對策：使用**802.11i雙向認證的功能**，可降低此威脅。有些廠商提供偵測此攻擊的偵測，除了發出告警訊息給管理者之外，並將攻擊者放入黑名單中。
- WEP弱點：
  - 弱點說明：透過明碼進行傳送、使用靜態加密金鑰、缺少封包完整性的確認。
  - 因應對策：建議使用**WPA2**來取代WEP。某些廠商提供WEP弱點的設備，產生告警資訊，提供資訊人員後續處理依據。





# 無線網路資安問題

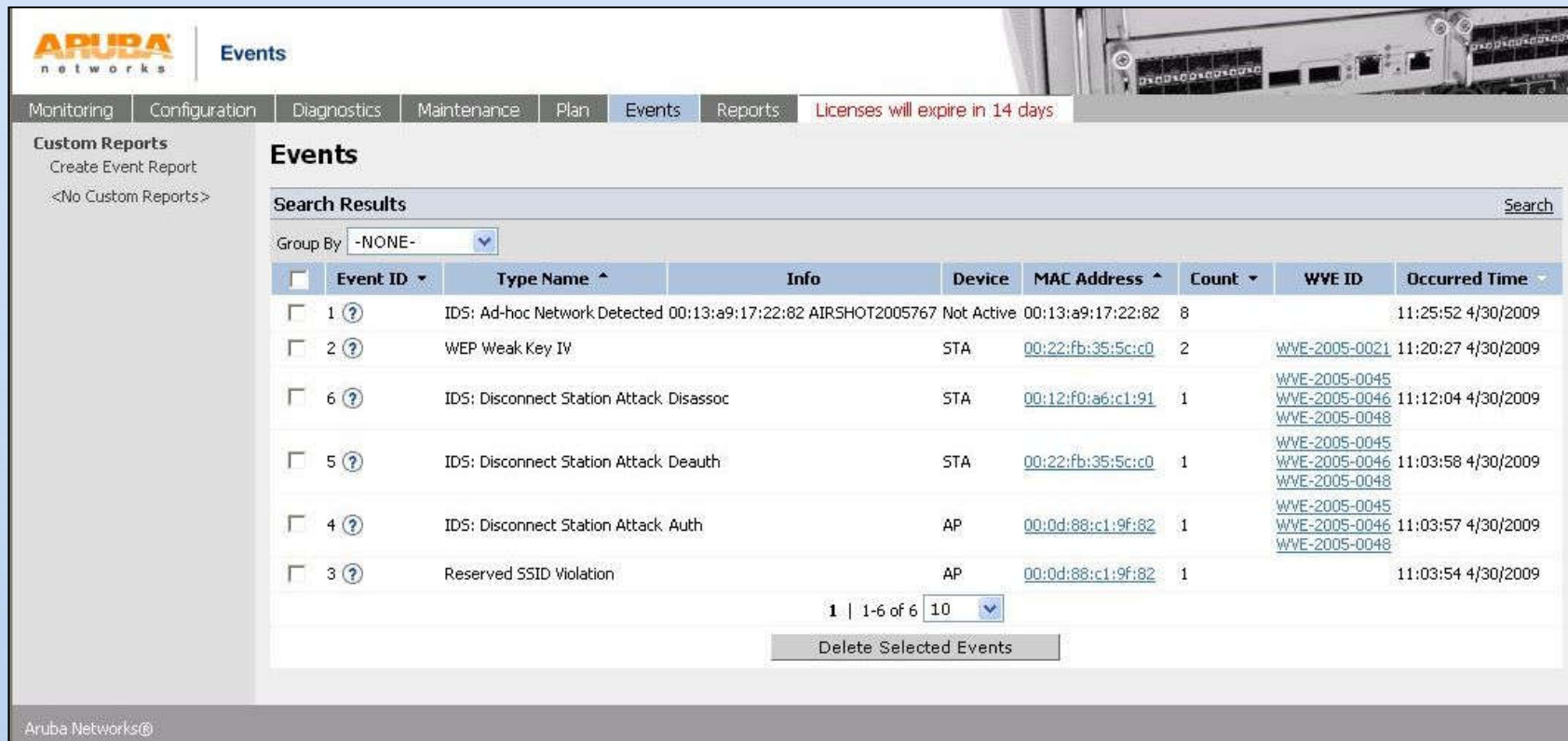
## 廠商可提供的解決方案

	Aruba	Cisco	D-Link	FON
1. 竊聽(Eavesdropping)				
2. 流量分析(Traffic Analysis )				
3. 偽裝(Masquerade)				
4. 重播(Replay )	●			
5. 訊息竄改(Message modification)				
6. 通訊劫奪(Session Hijacking)	●			
7. 阻斷服務(Denial-Of-Services)	●	●	●	
8. 中間攻擊(Main-in-the-Middle)	●			
9. WEP弱點	●			



# 無線網路資安問題

## 中間攻擊及WEP弱點測試



The screenshot displays the Aruba Networks Events page. The top navigation bar includes Monitoring, Configuration, Diagnostics, Maintenance, Plan, Events, and Reports. A notification indicates that licenses will expire in 14 days. The left sidebar shows options for Custom Reports, including 'Create Event Report' and '<No Custom Reports>'. The main content area is titled 'Events' and features a search bar and a 'Group By' dropdown set to '-NONE-'. Below this is a table of search results with columns for Event ID, Type Name, Info, Device, MAC Address, Count, WVE ID, and Occurred Time. The table lists six events, with the first event having a count of 8. At the bottom of the table, there is a pagination control showing '1 | 1-6 of 6' and a 'Delete Selected Events' button.

<input type="checkbox"/>	Event ID	Type Name	Info	Device	MAC Address	Count	WVE ID	Occurred Time
<input type="checkbox"/>	1	IDS: Ad-hoc Network Detected	00:13:a9:17:22:82 AIRSHOT2005767 Not Active	Not Active	00:13:a9:17:22:82	8		11:25:52 4/30/2009
<input type="checkbox"/>	2	WEP Weak Key IV		STA	<a href="#">00:22:fb:35:5c:c0</a>	2	<a href="#">WVE-2005-0021</a>	11:20:27 4/30/2009
<input type="checkbox"/>	6	IDS: Disconnect Station Attack Disassoc		STA	<a href="#">00:12:f0:a6:c1:91</a>	1	<a href="#">WVE-2005-0045</a> <a href="#">WVE-2005-0046</a> <a href="#">WVE-2005-0048</a>	11:12:04 4/30/2009
<input type="checkbox"/>	5	IDS: Disconnect Station Attack Deauth		STA	<a href="#">00:22:fb:35:5c:c0</a>	1	<a href="#">WVE-2005-0045</a> <a href="#">WVE-2005-0046</a> <a href="#">WVE-2005-0048</a>	11:03:58 4/30/2009
<input type="checkbox"/>	4	IDS: Disconnect Station Attack Auth		AP	<a href="#">00:0d:88:c1:9f:82</a>	1	<a href="#">WVE-2005-0045</a> <a href="#">WVE-2005-0046</a> <a href="#">WVE-2005-0048</a>	11:03:57 4/30/2009
<input type="checkbox"/>	3	Reserved SSID Violation		AP	<a href="#">00:0d:88:c1:9f:82</a>	1		11:03:54 4/30/2009

Aruba Networks®





## 各廠商佈建成本比較

# Aruba AP

項 目	單 價	數 量	價 格
Controller (含384台AP授權，每個Module最大可擴充至512台AP)	2,110,847	1	2,110,847
加購一片Modules(中信局無)	1,889,650	1	1,889,650
128個AP授權(中信局無)	571,200	1	571,200
512個AP授權(中信局無)	2,056,600	1	2,056,600
AP	14,819	1,000	14,819,000
合計(可同時2048人上網)			21,447,297



# 各廠商佈建成本比較

PART NUMBER	DESCRIPTION		台幣訂價 \$NTD
<b>Remote Access Point Software</b>			
ARUBA REMOTE ACCESS POINT SOFTWARE is an optional addition to ArubaOS functionality that supports secure remote deployment of Aruba Access Points over a untrusted (internet) WAN. These modules can be added through a software upgrade to any Supervisor Card			
LIC-1-RAP-3	Remote Access Point License (Single Access Point License)-3 Year	D	8,750
LIC-4-RAP-3	Remote Access Point License (4 Access Point License)-3 Year	D	35,000
LIC-6-RAP-3	Remote Access Point License (6 Access Point License)-3 Year	D	42,000
LIC-8-RAP-3	Remote Access Point License (8 Access Point License)-3 Year	D	52,500
LIC-16-RAP-3	Remote Access Point License (16 Access Point License)-3 Year	D	98,000
LIC-24-RAP-3	Remote Access Point License (24 Access Point License)-3 Year	D	140,000
LIC-48-RAP-3	Remote Access Point License (48 Access Point License)-3 Year	D	245,000
LIC-64-RAP-3	Remote Access Point License (64 Access Point License)-3 Year	D	280,000
LIC-128-RAP-3	Remote Access Point License (128 Access Point License)-3 Year	D	525,000
LIC-256-RAP-3	Remote Access Point License (256 Access Point License)-3 Year	D	840,000
<b>ARUBA M3 SOFTWARE</b>			
<b>ARUBA M3 Software Options</b>			
LIC-128-AP-3	Access Point License (128 Access Point License)-3 Year	SW	571,200
LIC-256-AP-3	Access Point License (256 Access Point License)-3 Year	SW	1,085,700
LIC-384-AP-3	Access Point License (384 Access Point License)-3 Year	SW	1,585,500
LIC-512-AP-3	Access Point License (512 Access Point License)-3 Year	SW	2,056,600
LIC-WIP-128-3	Wireless Intrusion Protection Module License (128 AP Support)-3 Year	SW	400,400
LIC-WIP-256-3	Wireless Intrusion Protection Module License (256 AP Support)-3 Year	SW	721,000
LIC-WIP-384-3	Wireless Intrusion Protection Module License (384 AP Support)-3 Year	SW	1,021,300
LIC-WIP-512-3	Wireless Intrusion Protection Module License (512 AP Support)-3 Year	SW	1,281,700
LIC-PEF-2048-3	Policy Enforcement Firewall Module License (2048 Users)-3 Year	SW	952,000
LIC-PEF-4096-3	Policy Enforcement Firewall Module License (4096 Users)-3 Year	SW	1,713,600
LIC-PEF-8192-3	Policy Enforcement Firewall Module License (8192 Users)-3 Year	SW	3,046,400
LIC-VOC-2048-3	Voice Services Module License (2048 Users)-3 Year	SW	714,000
LIC-VOC-4096-3	Voice Services Module License (4096 Users)-3 Year	SW	1,285,200
LIC-VOC-8192-3	Voice Services Module License (8192 Users)-3 Year	SW	2,284,800
LIC-VPN-2048-3	VPN Server Module License (2048 Sessions)-3 Year	SW	856,800
LIC-VPN-4096-3	VPN Server Module License (4096 Sessions)-3 Year	SW	1,542,800
LIC-VPN-8192-3	VPN Server Module License (8192 Sessions)-3 Year	SW	2,741,900
LIC-XSC-2048-3	xSec Module License (2048 Sessions)-3 Year	SW	952,000
LIC-XSC-4096-3	xSec Module License (4096 Sessions)-3 Year	SW	1,713,600
LIC-XSC-8192-3	xSec Module License (8192 Sessions)-3 Year	SW	3,046,400



## 各廠商佈建成本比較

# Cisco AP

項 目	單 價	數 量	價 格
管理軟體(一千台授權,中信局無)	2,000,000	1	2,000,000
6500 模組可管300台AP(需有Super720 Module , 中信局無)	1,150,000	4	4,600,000
AP	9,448	1,000	
合計			16,048,000
管理軟體(一千台授權,中信局無)	2,000,000	1	2,000,000
6504機箱(含一片模組可管300台AP)	1,918,977	2	3,837,954
加購一片模組(中信局無)	1,000,000	2	2,000,000
AP	9,448	1,000	9,448,000
合計			17,285,954
管理軟體(一千台授權,中信局無)	2,000,000	1	2,000,000
獨立式 Controller(可管100台AP)	1,044,776	10	10,447,760
AP	9,448	1,000	9,448,000
合計			21,895,760

## 各廠商佈建成本比較

# D-Link Thin AP

項 目	單 價	數 量	價 格
Controller(每台可管48台AP及512人同時上網，最多堆疊可管192台AP及同時2048人上網)	127,932	44	5,629,008
AP	11,275	1,000	11,275,000
管理軟體(管理所有Controller, 中信局無)	500,000	1	500,000
合計			17,404,008



## 各廠商佈建成本比較

# D-Link Fat AP

項 目	單 價	數 量	價 格
Gateway(可同時120人上網)	37,643	30	1,129,290
Gateway(可同時500人上網)	120,000	14	1,680,000
AP	5,544	1,000	5,544,000
合計			8,353,290





## 各廠商佈建成本比較

# FON AP

項 目	單 價	數 量	價 格
Controller(可管理100台AP，中信局無)	186,470	10	1,864,700
AP(中信局無)	11,310	1000	11,310,000
合計			13,174,700

