

台北海洋技術學院

Taipei College of Maritime Technology

103 年 ISO-Insight 教育訓練



時間:103 年 3 月 28 日下午 13:00~17:00

地點:台北海洋技術學院圖書館會議室

講師: 王智民 先生

ISOinsight 簡易操作設定

台北海洋技術學院

大綱

- * 簡報說明(30min)
 - * 環境設定與基本設定
 - * 主要使用功能介紹
- * 實際畫面操作說明(60min)
 - * 操作實際設備，逐項說明
- * 問題討論與回覆(30min)

環境設定

本機設定(登入)

登入IP: 172.22.253.252(可以直接在瀏覽器上打IP)

IsOinsight

172.22.253.252/isoinsight/isosys1024.php

Username = admin
Password = xxxxxxxx

點選此處直接進入公佈欄

帳號:
密碼:
認證方式: InternalDB | 終端設備: Other PC
版本: v2.7.1.A1.20130905
狀態:

授權用戶: 海洋技術學院

授權內容	設備	終端	流量IP	AD身份	資產
正式版授權數	200	64	0	0	0

更改IP

系統管理 -> 網路與介面 -> 本機網路介面設定可以設定設備的IP等

Rote: 設定該port類型 (Mng:管理, Lsn:收ARP封包, Mirrio:收流量 不需要設定IP)

本機網路介面設定

注意! 更改IP會重新開機

更改介面設定

網路設定

網際IP: 172.22.253.254
DNS伺服器IP: 140.129.255.2
v6網際IP:
v6DNS伺服器IP:
Domain Name: comt.edu.tw

本機介面設定

介面名稱	IP地址	子網掩碼	v6 IP	v6子網掩碼	VLAN ID	Role	Tag	Boast計算	啟用
Eth0	172.22.253.252	255.255.255.0			1	Mng+Lsn	Untag	Enable	Enable
Eth1					1	Mng+Lsn	Untag	Enable	Disable
Eth2					1	Mng+Lsn	Untag	Enable	Disable
Eth3					1	Mng+Lsn	Untag	Enable	Disable
Eth4					1	Mng+Lsn	Untag	Enable	Disable
Eth5					1	Mng+Lsn	Untag	Enable	Disable
Eth6					1	Mng+Lsn	Untag	Enable	Disable

注意! 有用到的port需Enable

時間設定

設定正確的時間會跟資料正確性有關係

本機系統時間設定

儲存

時間

目前時間: 2014/03/26 10:50:08

系統時間設定

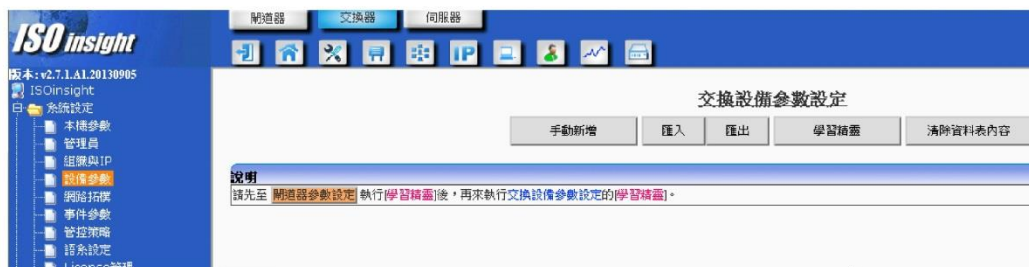
修改時間為: 年 月 日 時 分 更改時間

修改時區: +8
修改NTP伺服器: 172.22.253.254 立刻NTP同步

功能設定說明

定義物件

- * 剛開始設定好環境基本參數(IP, 時間等),就可以開始新增網路環境中的基本設備
- * ISOinsight 主要監控的設備有, 閘道器、交換器、伺服器、電腦主機、AP等可以透過學習精靈或手動的方式新增
- * 透過學習精靈學到的設備會自動加入拓撲圖中



閘道器

網路中如有多個Vlan就需加入, 影響MAC鎖定及Vlan, IP使用歷史相關資料
學習精靈必要條件: **SNMP**

閘道器參數設定

手動新增 匯入 匯出 **學習精靈** 清除資料表內容

學習精靈列表

序號	網道器IP	網道器MAC	遠端
1	192.168.10.254	0026140003ca	255.255.255.0
2	192.168.11.254	98a7328fa600	255.255.255.0
3	192.168.12.254	98a7328fa600	255.255.255.0

原道器參數學習

說明: 本功能可自動學習網道器IP, 並將其加入學習列表。
說明: 選擇IP和MAC地址後, 即可自動學習。
• Gateway/Router IP - 網道器 IP (Gateway/Router 的 IP)
• VLAN ID - 網道器 Core system 的 VLAN ID (網道器 Core system 的 VLAN ID) (網道器 Core system 的 VLAN ID) (網道器 Core system 的 VLAN ID)

下一步 取消

操作條件設定

項目	條件	條件值
Gateway/Router IP	192.168.10.254	
Community	public	
VLAN ID		

學習完成!

閘道器參數學習

說明: 本功能可自動學習網道器IP, 並將其加入學習列表。
說明: 選擇IP和MAC地址後, 即可自動學習。

上一步 完成 取消

項目	序號	IP	MAC	MASK	VlanID
1	☐	192.168.10.254	98a7328fa600	255.255.255.0	10
2	☐	192.168.11.254	98a7328fa600	255.255.255.0	11
3	☐	192.168.12.254	98a7328fa600	255.255.255.0	12
4	☐	192.168.13.254	98a7328fa600	255.255.255.0	13
5	☐	192.168.14.254	98a7328fa600	255.255.255.0	14
6	☐	192.168.15.254	98a7328fa600	255.255.255.0	15
7	☐	192.168.16.254	98a7328fa600	255.255.255.0	16
8	☐	192.168.17.254	98a7328fa600	255.255.255.0	17
9	☐	192.168.18.254	98a7328fa600	255.255.255.0	18
10	☐	192.168.19.254	98a7328fa600	255.255.255.0	19

交換器

影響switch port鎖定, 定位資訊
學習精靈必要條件: **SNMP**

交換器參數設定

手動新增 匯入 匯出 **學習精靈** 清除資料表內容

學習精靈列表

序號	交換器IP	交換器MAC	遠端
1	192.168.10.254	0026140003ca	255.255.255.0
2	192.168.11.254	98a7328fa600	255.255.255.0
3	192.168.12.254	98a7328fa600	255.255.255.0

原道器參數學習

說明: 本功能可自動學習網道器IP, 並將其加入學習列表。
說明: 選擇IP和MAC地址後, 即可自動學習。
• Gateway/Router IP - 網道器 IP (Gateway/Router 的 IP)
• VLAN ID - 網道器 Core system 的 VLAN ID (網道器 Core system 的 VLAN ID) (網道器 Core system 的 VLAN ID)

下一步 取消

操作條件設定

項目	條件	條件值
Gateway/Router IP	192.168.10.254	
Community	public	
VLAN ID		

學習完成!

交換器參數學習

說明: 本功能可自動學習網道器IP, 並將其加入學習列表。
說明: 選擇IP和MAC地址後, 即可自動學習。

上一步 完成 取消

項目	序號	IP	MAC	MASK	VlanID
1	☐	192.168.10.254	98a7328fa600	255.255.255.0	10
2	☐	192.168.11.254	98a7328fa600	255.255.255.0	11
3	☐	192.168.12.254	98a7328fa600	255.255.255.0	12
4	☐	192.168.13.254	98a7328fa600	255.255.255.0	13
5	☐	192.168.14.254	98a7328fa600	255.255.255.0	14
6	☐	192.168.15.254	98a7328fa600	255.255.255.0	15
7	☐	192.168.16.254	98a7328fa600	255.255.255.0	16
8	☐	192.168.17.254	98a7328fa600	255.255.255.0	17
9	☐	192.168.18.254	98a7328fa600	255.255.255.0	18
10	☐	192.168.19.254	98a7328fa600	255.255.255.0	19

手動設定設備

開通器 交換器 伺服器																	
請先至 開通器參數設定 執行(學習新畫)後，再來執行交換設備參數設定的(學習新畫)。																	
詳細單位																	
交換設備列表																	
序號	IP位址	主機名稱	設備種類	埠	唯讀權限	修改權限	SNMP版本	位置	連結	群組	介面數量	上行介面	下行介面	輪詢	設備ID	設備PW	作業項目
1.	172.22.24.201	福環A_1樓_POE	其他	161	public		V1		172.22.24.201		225	4,2,6		是			↗
2.	172.22.24.202	福環A_2樓_POE	其他	161	public		V1		172.22.24.202		225	7,2,13,16,24,20		是			↗
3.	172.22.24.203	福環A_5樓_POE	其他	161	public		V1		172.22.24.203		225	6,3,12,5		是			↗
4.	172.22.24.204	福環A_8樓_POE	其他	161	public		V1		172.22.24.204		225	11,5,14,6		是			↗
5.	172.22.24.205	福環B_2樓_POE	其他	161	public		V1		172.22.24.205		225	4		是			↗
6.	172.22.24.206	福環B_5&6樓_POE	其他	161	public		V1		172.22.24.206		225			是			↗
7.	172.22.24.207	體育館_POE	其他	161	public		V1		172.22.24.207		225	6		是			↗
8.	172.22.24.208	宿舍大樓_POE	其他	161	public		V1		172.22.24.208		225			是			↗
9.	172.22.24.209	CH_B1A	其他	161	public		V1		172.22.24.209		28			是			↗
10.	172.22.24.210	CH_B1C	其他	161	public		V1		172.22.24.210		225	8		是			↗
11.	172.22.24.211	CH_1FA	其他	161	public		V1		172.22.24.211		28	1		是			↗
12.	172.22.24.212	CH_1FC	其他	161	public		V1		172.22.24.212		24	5,3		是			↗
13.	172.22.24.213	CH_3FA	其他	161	public		V1		172.22.24.213		28			是			↗
14.	172.22.24.214	CH_3FC	其他	161	public		V1		172.22.24.214		24	10		是			↗
15.	172.22.24.215	CH_4FA	其他	161	public		V1		172.22.24.215		28			是			↗
16.	172.22.24.216	CH_4FC	其他	161	public		V1		172.22.24.216		24	4		是			↗
17.	172.22.253.253	Ruckus	其他	161	public		V2C		https://172.22.253.253					是			↗
18.	172.22.253.254	HP-7506	其他	161	public		V2C		http://172.22.253.254					是			↗

拓樸圖設置

以樹狀結構定義拓樸圖連結方式,精靈學習完這邊會有基本幫你建上去的
若無法透過學習取得或非SNMP設備也可以手動增加

綠色+: 平行新增物件, 黃色+: 新增子物件, 紅色-: 刪除物件

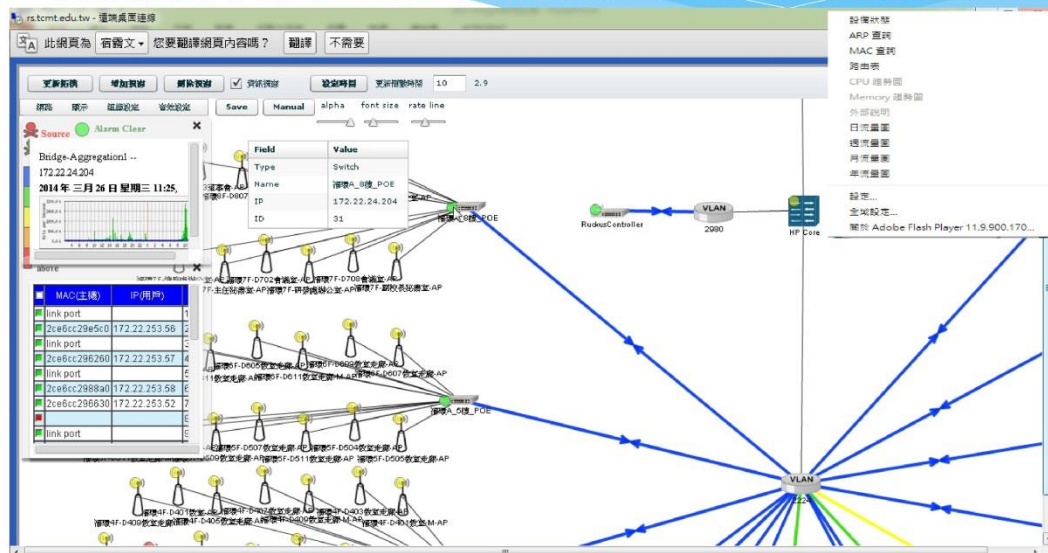
拓本: v2.7.1.1.1.3018065																	
ISOinsight																	
系統設定																	
■ 系統參數																	
■ 管理員																	
■ 組網與IP																	
■ 設備參數																	
■ 網路拓樸																	
■ 事件參數																	
■ 監控策略																	
■ 語法設定																	
■ License管理																	
■ 網路監視																	
■ MAC/IP管理																	
■ 整合AD認證																	
■ 流量分析																	
■ 事件管理																	
儲存																	
網路拓樸列表																	
路由		路由	名稱	IP Core	管理 IP	172.22.253.254	上行介面		流量圖輔助設定	門限(4b)	100000	VLAN_OID					
VLAN		VLAN	名稱	2224	Gateway IP	172.22.24.254	介面		流量圖輔助設定	門限(4b)	100000						
交換器		交換器	名稱	福環A_1樓_POE	管理 IP	172.22.24.201	上行介面	225	流量圖輔助設定	門限(4b)	10000						
無線基地台		無線基地台	名稱	福環1F-學務處辦公室	管理 IP	172.22.253.6	上行介面		流量圖輔助設定	門限(4b)	10000						
無線基地台		無線基地台	名稱	福環1F-學務處辦公室	管理 IP	172.22.253.7	上行介面		流量圖輔助設定	門限(4b)	10000						
無線基地台		無線基地台	名稱	福環B1F-停車場G2-AP	管理 IP	172.22.253.62	上行介面		流量圖輔助設定	門限(4b)	10000						
無線基地台		無線基地台	名稱	福環B1F-停車場G3-AP	管理 IP	172.22.253.63	上行介面		流量圖輔助設定	門限(4b)	10000						
無線基地台		無線基地台	名稱	福環B1F-停車場G4-AP	管理 IP	172.22.253.64	上行介面		流量圖輔助設定	門限(4b)	10000						
無線基地台		無線基地台	名稱	福環B1F-停車場G5-AP	管理 IP	172.22.253.65	上行介面		流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環A_2樓_POE	管理 IP	172.22.24.202	上行介面	225	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環A_5樓_POE	管理 IP	172.22.24.203	上行介面	225	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環A_8樓_POE	管理 IP	172.22.24.204	上行介面	225	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環B_2樓_POE	管理 IP	172.22.24.205	上行介面	225	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環B_5&6樓_POE	管理 IP	172.22.24.206	上行介面	225	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	體育館_POE	管理 IP	172.22.24.207	上行介面	225	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環A_1樓_POE	管理 IP	172.22.24.208	上行介面	28	流量圖輔助設定	門限(4b)	10000						
交換器		交換器	名稱	福環B_1樓_POE	管理 IP	172.22.24.210	上行介面	225	流量圖輔助設定	門限(4b)	10000						

設定後資料查詢與監控

拓樸圖

設置完成就可以看到此視窗可點選資訊視窗看更詳細內容(流量, port接誰等)

綠色燈號:無事件發生, 黃色燈號:今天有發生過事件, 紅色:一小時內發生事件



交換機狀態

設置完成就可以看到此視窗 可以透過畫面確認每台交換機設備的狀態



交換機流量圖

設置完成就可以看到此視窗 可點選展開後看更詳細內容(流量...等)



事件觸發郵件設定

設定管理者當事件觸發時可以自動通知

SO insight
版本: v2.7.1.LAL20130905
ISOnsight

系統設定
■ 系統參數
■ 管理員
■ 組織與IP
■ 設備參數
■ 網絡拓撲
■ 事件參數
■ 監控策略
■ 策略設定
■ License管理
■ 網絡監視
■ MAC/IP管理
■ 整合AD認證
■ 流量分析
■ 事件管理

事件觸發 顯示設定

儲存

事件正規化

日誌事件觸發間隔時間	分鐘(空白表示預設 5分鐘)
觸發等級	等級 0 為最高嚴重等級(空白表示預設等級 4)
同性質重複日誌合併事件	小時(空白表示預設 4小時)內視同一事件
觸發事件解決後是否重新計算	是 (預設是)

Syslog轉送

異常事件是否發送至 Log Server IP: (空白表示No)

電子郵件通知設定

電子郵件伺服器網址(IP): bgic

電子郵件伺服器Port: 25

郵件寄送者顯示: sysmang@mail.tcmf.edu.tw

SMTP登入帳號: sysmang@mail.tcmf.edu.tw

SMTP登入帳號密碼: *****

接受通知者的電子郵件地址:

1. sysmang@mail.tcmf.edu.tw
2. bgiclog@bgic.com.tw
3. joe@bgic.com.tw

事件觸發與事件管理

事件觸發設定可以定義或新增特定事件，並決定該事件發生時採用何種動作

ISU insight

版本: v2.7.1.LAL20130905

ISOnsight

系統設定

■ 系統參數

■ 管理員

■ 組織與IP

■ 設備參數

■ 網絡拓撲

■ 事件參數

■ 監控策略

■ 策略設定

■ License管理

■ 網絡監視

■ MAC/IP管理

■ 整合AD認證

■ 流量分析

■ 事件管理

6	啟用設備異常	A43_Cisco_StormControl	Cisco	1	%STORM_CONTROL	disable	disable	0	Y	N	MsgOnly	Cisco交換器發現廣播暴風
7	啟用設備異常	A45_Cisco_VLAN_MISMATCH	Cisco	1	VLAN_MISMATCH	disable	disable	0	Y	N	MsgOnly	Cisco交換器發現不實VLAN事件
8	啟用設備異常	A46_NBADswitch 3 事件	NBADswitch	2	[NS-29900-26] ARP Spoofing Prevention	disable	disable	0	Y	Y	MsgOnly	NBAD 29800 事件
9	啟用設備異常	A47_NBADswitch 3 事件	NBADswitch	2	[NS-29900-26] ARP (Pscan Limit Control	disable	disable	0	Y	Y	MsgOnly	NBAD 29800 事件
10	啟用設備異常	A48_Abocom_EventLog	Abocom	3	<134> WAN	disable	disable	0	Y	N	MsgOnly	Abocom Firewall WAN 連線事
11	啟用設備異常	A50_監控廠商異常	NBADmanager1	1	log_id=nbad0001,attack_id=10000012	disable	disable	0	Y	Y	MsgOnly	阿摩騰TCP服務反惡意掃描事件
12	啟用Ruckus_APAP CPU使用率過高	其他	2	AP cpu utilization is too high.	disable	disable	0	Y	Y	MsgOnly	AP CPU使用率過高	
13	啟用地址異常	B11_Rogue DHCP	NBADsensor	2	log_id=nbad0001,attack_id=10000015	手動	MAC	30	Y	N	MsgOnly	偵測到非法DHCP server
14	啟用地址異常	B12_ARP 異常	NBADsensor	2	log_id=nbad0001,attack_id=10000001	手動	Port	120	N	N	MsgOnly	偵測到非法ARP封包
15	啟用地址異常	B13_ARP廣播分析(5分)	NBADsensor	2	VLAN 臨界值 5000 次 / 5分鐘	手動	Port	120	N	N	MsgOnly	VLAN(5分鐘)廣播數量累積超過
16	啟用地址異常	B14_ARP廣播分析(5分)	NBADsensor	2	臨界值 500 次 / 5秒	手動	Port	120	N	N	MsgOnly	單一IP(5秒)廣播數量累積超過
17	啟用地址異常	B15_ARP_IP_Scan	NBADsensor	2	IPScan臨界值 500 次 / 秒	手動	MAC	120	N	N	MsgOnly	偵測到IPscan掃描
18	停用地址異常	B17_IP-MAC綁定	NBADsensor	1	預設動作 拒絕	手動	MAC	120	N	N	MsgOnly	MAC/IP不符合監控策略
19	啟用地址異常	B18_ARP_Replay 異常	NBADsensor	3	錯誤封包數 > 3 個	disable	disable	0	Y	N	MsgOnly	ARP回覆錯誤封包 - 臨界值
20	停用地址異常	B19_IP-MAC-PORT綁定	NBADsensor	1	偵測封包等待時間 5 分鐘	手動	MAC	10	N	N	MsgOnly	MAC/IP/PORT不符合監控策略
21	啟用身份異常	C41_Cisco ACS Server	Cisco	3	<181>	disable	disable	0	Y	N	MsgOnly	Cisco ACS 認證記錄
22	啟用行為異常	D10_目的主機數分析	NBADanalyzer1	1	目的主機數臨界值 500 主機 / 5分鐘	手動	Port	120	N	N	MsgOnly	用戶目的主機訪問數超過臨界值
23	啟用行為異常	D11_目的埠數分析	NBADanalyzer2	2	目的埠數臨界值 500 埠 / 5分鐘	手動	Port	120	N	N	MsgOnly	用戶目的埠訪問數超過臨界值
24	啟用行為異常	D12_目的會談數分析	NBADanalyzer2	2	目的會談數臨界值 5000 會談 / 5分鐘	手動	Port	120	N	N	MsgOnly	用戶目的訪問會談數超過臨界值
25	啟用行為異常	D13_流量分析	NBADanalyzer2	2	流量限制 3000 Mbytes / 日	手動	Port	1440	N	N	MsgOnly	用戶使用流量超過每日額度
26	啟用行為異常	D14_病毒規則分析	NBADanalyzer1	1	log_id=nbad0001,attack_id=10000004	手動	Port	1440	N	N	MsgOnly	發現用戶會談行為疑似病毒事件
27	啟用Ruckus_APSSID衝突	其他	2	A new SSID-spoofing	disable	disable	0	Y	Y	MsgOnly	SSID衝突	
28	啟用Ruckus_AP未連線	其他	4	(Ap) heartbeats lost	disable	disable	0	Y	Y	MsgOnly	未連線	
29	啟用Ruckus_AP連線中斷	其他	2	Lost contact with (ap)	disable	disable	0	Y	Y	MsgOnly	連線中斷	
30	啟用Ruckus_AP超過最大Client數	其他	2	(ap)'s online client number is (value) which exceeds	disable	disable	0	Y	Y	MsgOnly	超過最大Client數	

事件查詢

ISO insight

版本: v2.7.1.A1.20130905

ISO insight

系統設定

- 系統參數
- 管理員
- 組網與IP
- 設備參數
- 網絡拓撲
- 事件參數
- 策略策略
- 策略設定
- License管理
- 網絡監控
- MAC/IP管理
- 安全策略
- 流量分析
- 事件管理

SYSLOG日誌 | SNMP trap | Incident事件 | 手動封鎖列表 | 封鎖列表 | 歷史封鎖列表

Syslog 查詢

清除記錄

過濾條件: 近1小時 或 今天 或 本星期 或 日期: 2014 / 03 / 26 10 : 46 至 2014 / 03 / 26 11 : 49

事件等級 訊息來源 來源IP 來源MAC 訊息

查詢條件: [] [] [] [] []

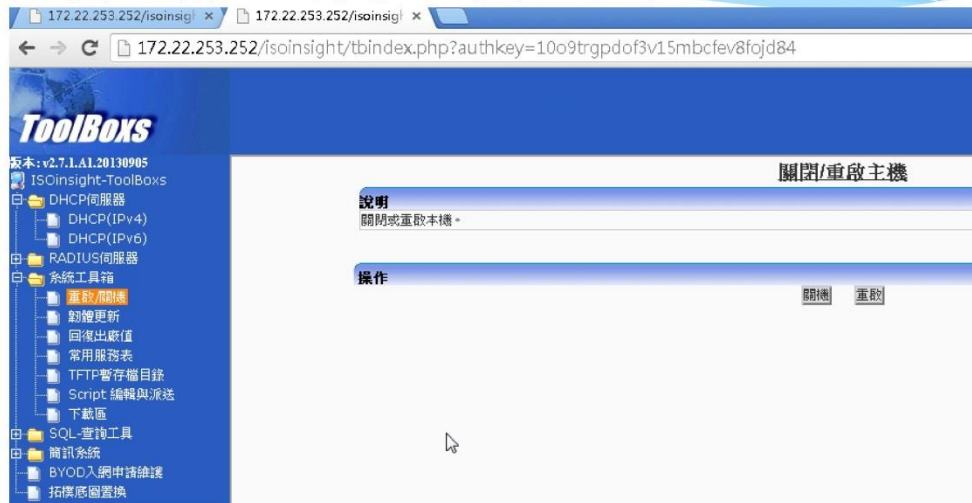
首頁 上頁 下頁 末頁 Goto [] 頁 共8703項記錄, 搜尋結果共1176頁, 本頁為第11頁 Down

編號	事件等級	訊息來源	來源IP	來源MAC	日期時間	訊息
1.	info	172.22.253.253			20140326 11:48:52	~134-Mar 26 11:53:00 syslog: eventId_to_syslog0:User[34:35:0a:b5:c6:65] disconnects from VLAN[TCMT-wlan] at AP[CS-3F-B305@2c:e6:cc:28:dc:00]
2.	info	172.22.253.253			20140326 11:48:52	~134-Mar 26 11:53:00 syslog: eventId_to_syslog0:User[34:35:0a:b5:c6:65] leave VLAN[TCMT-wlan] at AP[CS-3F-B305@2c:e6:cc:28:dc:00] with Session Time[101.26 sec] RX Bytes[3884] TX Bytes[196369]
3.	info	172.22.253.146			20140326 11:48:52	~3> Mar 26 03:53:14 syslog: hwapo_wtp_end_dvc_type: data len = 0 != len = 164, msg_type = 40
4.	info	172.22.253.253			20140326 11:48:52	~134-Mar 26 11:53:00 syslog: eventId_to_syslog0:User[34:35:0a:b5:c6:65] joins VLAN[TCMT-wlan] from AP[CS-2F-A201@2c:e6:cc:28:42:d0]
5.	info	172.22.253.253			20140326 11:48:52	~134-Mar 26 11:53:00 syslog: eventId_to_syslog0:User[36:03:d9:93:00:c0] joins VLAN[TCMT-wlan] from AP[CS-5F-A501@2c:e6:cc:28:c5:60]

維護設定與備份

重啟、關機

可以在系統工具箱->重啟/關機裡面去讓機器重新啟動



資料備份

完成設定後可以將設定資料匯出備份，同樣可以在此畫面執行設定上傳還原



軟體更新

系統工具箱->韌體更新

當系統需要做更新時,可以當檔案放置於個人電腦中,透過網頁的方式上傳更新



實機畫面操作 與逐項說明

實機畫面操作後 問題討論

簽到單

博鈺資訊股份有限公司

網路實務研習營簽到表

日期：103 年 3 月 28 日下午 13:00~17:00

地點：台北海洋技術學院圖書館會議室

講師：王智民先生

[illegible]