

台北海洋技術學院

Taipei College of Maritime Technology

104 年 ISO-insight 教育訓練



時間:104 年 12 月 18 日下午 03:00~04:00

地點台北海洋技術學院淡水校區福環樓 6F D617 教室

講師:王智民先生

Netvision ISOInsight 無線網路管理系統教育訓練簽到表

[illegible]



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)

Username = admin
Password = xxxxxxxx

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)

172.22.253.252/isoinsight x

172.22.253.252/isoinsight/tempindex.php?authkey=2o9trgpdof3v15mbcf8fojd84

ISO insight

版本: v2.7.1.A1.20130905

ISOinsight

系統設定

- 本機參數
- 管理員
- 組織與IP
- 設備參數
- 網路拓樸
- 事件參數
- 管控策略
- 語系設定
- License管理

網路與介面 系統時間 資料備份 網路服務 系統狀態

本機網路介面設定

更改介面設定

網路設定

開道器IP	172.22.253.254	v6開道器IP		Domain Name	tcmt.edu.tw
DNS伺服器IP	140.129.255.2	v6DNS伺服器IP			

本機介面設定

介面名稱	介面IP	子網遮罩	V6 IP	V6子網遮罩	VLAN ID	Role	Tag	Bcast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

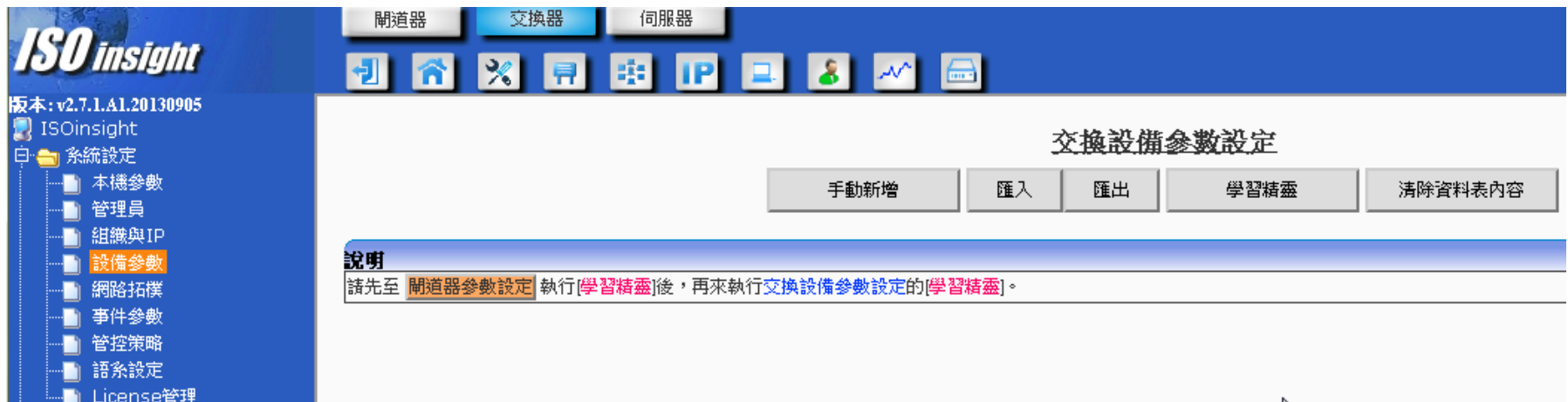
注意! 更改IP會重新開機

注意! 有用到的port需Enable

功能設定説明

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樸圖中



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

閘道器列表

序號	閘道器IP	閘道器MAC	遮罩
1.	192.168.10.254	00261400b3ca	255.255.255.0
2.	192.168.11.254	e8e7326fa600	255.255.255.0
3.	192.168.12.254	e8e7326fa600	255.255.255.0

閘道器參數學習

說明

勾選設定好操作條件後, 請按[下一步]繼續。
按[取消]將中斷學習精靈的學習過程。

- Gateway/Router IP -- 請輸入 Core switch 或 Router 的 IP
- VLAN OID -- 指的是 Core switch 或 Router 針對 VLAN 的物件識別碼(Object Identifier, 簡寫為OID), 如果指定的 Core switch 或 Router, 其 VLAN OID 並不是通用的 OID 時, 請填入該正確的非規則性 OID

下一步

取消

操作條件設定

Gateway/Router IP	192.168.10.234
Community	public
VLAN OID	

學習完成!

閘道器參數學習

說明

勾選要加入[閘道器參數]的項目後按[完成]儲存
按[取消]將中斷學習精靈的學習過程。

上一步

完成

取消

項目

##	☐	IP	MAC	MASK	VlanID
1.	☐	10.10.10.253	e8e7326fa600	255.255.255.0	10
2.	☐	10.30.254.254	e8e7326fa600	255.255.255.0	1
3.	☐	192.168.10.234	e8e7326fa600	255.255.255.0	1
4.	☐	192.168.11.254	e8e7326fa600	255.255.255.0	11
5.	☐	192.168.12.254	e8e7326fa600	255.255.255.0	12
6.	☐	192.168.13.254	e8e7326fa600	255.255.255.0	13
7.	☐	192.168.99.253	e8e7326fa600	255.255.255.0	99
8.	☐	192.168.101.253	e8e7326fa600	255.255.255.0	101
9.	☐	192.168.102.253	e8e7326fa600	255.255.255.0	102
10.	☐	192.168.103.253	e8e7326fa600	255.255.255.0	103

交換器

影響switch port鎖定, 定位資訊

學習精靈必要條件: **SNMP**

交換設備參數設定

手動新增 匯入 匯出 學習精靈 清除資料表內容

說明
請先至 [開通器參數設定](#) 執行[學習精靈]後, 再來執行交換設備參數設定的[學習精靈]。

詳細欄位

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.	192.168.10.13	Switch192.168.10.13	其他	161	public		V1		192.168.10.13		388	387		是			?
2.	192.168.10.14	Switch192.168.10.14	其他	161	public		V1		192.168.10.14		944	921,897		是			?
3.	192.168.10.15	Switch192.168.10.15	其他	161	public		V1		192.168.10.15		944	929,927,939,904,906,923,938,897		是			?
4.	192.168.10.200	Kenny-Test-Switch	Alcatel	161	public		V1							是			?
5.	192.168.10.234	Switch	其他	161	public		V1		192.168.10.234		24	11,1,13,19,23,14,16		是			?
6.	192.168.10.235	Switch192.168.10.235	其他	161	public		V1		192.168.10.235		48	3,7,6,2,23		是			?
7.	192.168.10.239	Switch192.168.10.239	其他	161	public		V1		192.168.10.239		1	2,24,9		是			?
										0,253	9	0		是			?

下一步 取消

操作條件設定

##	☐	VLAN IP	VLAN ID	Community
1.	☒	192.168.10. 1 ~ 254	1	public
2.	☐	192.168.11. 1 ~ 254	11	public
3.	☐	192.168.12. 1 ~ 254	12	public

詳細欄位

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.	192.168.10.13	Switch192.168.10.13	其他	161	public		V1		192.168.10.13		388	387		是			?
2.	192.168.10.14	Switch192.168.10.14	其他	161	public		V1		192.168.10.14		944	921,897		是			?
3.	192.168.10.15	Switch192.168.10.15	其他	161	public		V1		192.168.10.15		944	929,927,939,904,906,923,938,897		是			?
4.	192.168.10.200	Kenny-Test-Switch	Alcatel	161	public		V1							是			?
5.	192.168.10.234	Switch	其他	161	public		V1		192.168.10.234		24	11,1,13,19,23,14,16		是			?
6.	192.168.10.235	Switch192.168.10.235	其他	161	public		V1		192.168.10.235		48	3,7,6,2,23		是			?
7.	192.168.10.239	Switch192.168.10.239	其他	161	public		V1		192.168.10.239		1	2,24,9		是			?
8.	192.168.10.253	OAW4306	其他	161	public		V2C		192.168.10.253	9	0			是			?
9.	192.168.10.254	Switch192.168.10.254	其他	161	public		V1		192.168.10.254					是			?
10.	192.168.10.42	Switch192.168.10.42	其他	161	public		V1		192.168.10.42		23	19,15,17		是			?
11.	192.168.10.47	Switch192.168.10.47	其他	161	public		V1		192.168.10.47		1			是			?
12.	192.168.10.91	Switch	其他	161	public		V1		192.168.10.91		1	2,24		是			?
13.	192.168.10.97	Switch192.168.10.97	其他	161	public		V1		192.168.10.97		1			是			?

手動設定設備

閘道器

交換器

伺服器



請先至 [閘道器參數設定](#) 執行[學習精靈](#)後，再來執行[交換設備參數設定](#)的[學習精靈](#)。

詳細欄位

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

版本: v2.7.1.A1.20130905

ISOinsight

系統設定

- 本機參數
- 管理員
- 組織與IP
- 設備參數
- 網路拓樸
- 事件參數
- 管控策略
- 語系設定
- 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

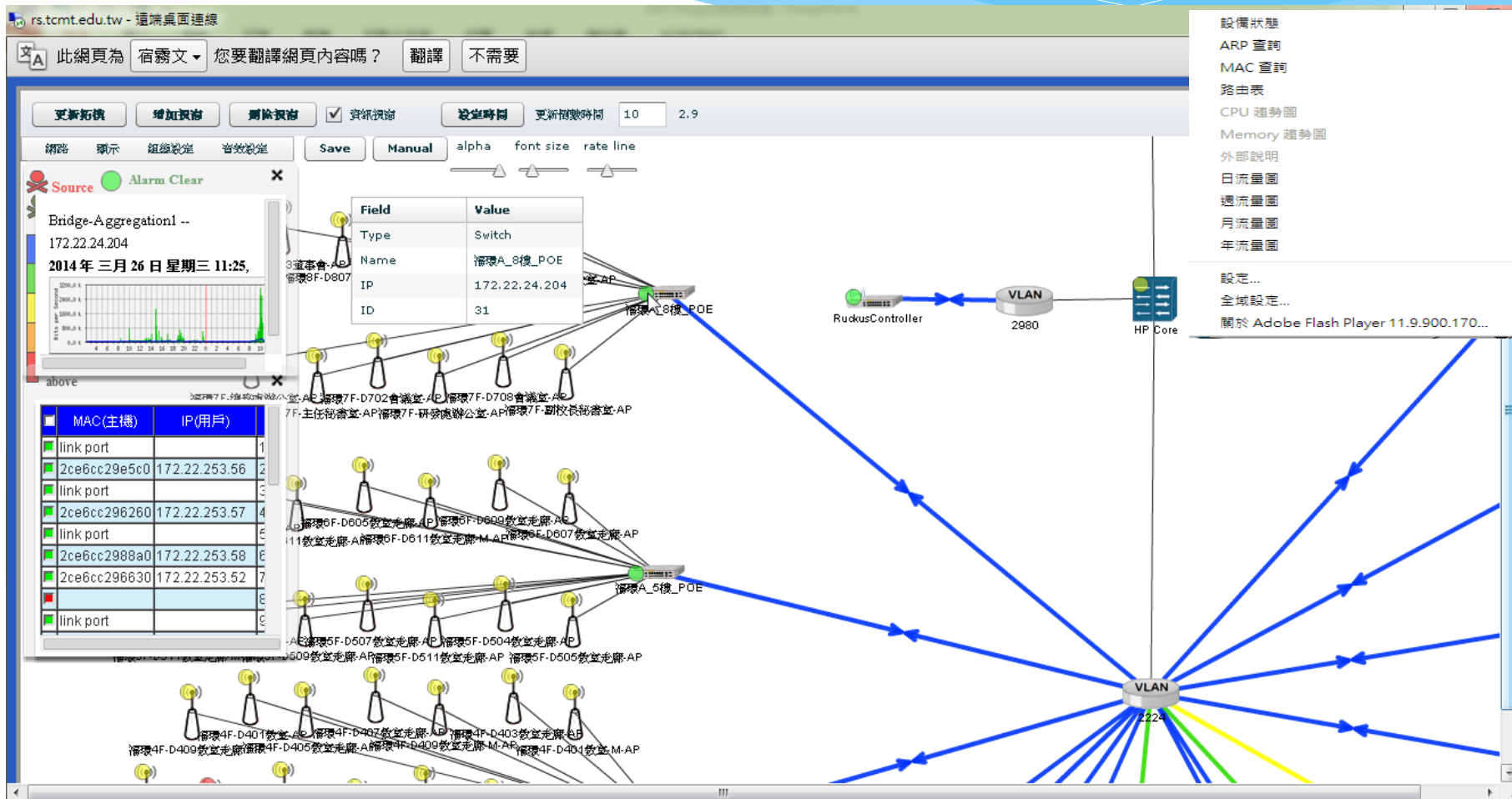
路由器	名稱	HP Core	管理 IP	172.22.253.254	上行介面		流量圖細節設定	門檻(kb)	100000	VLAN_OID		+
VLAN	名稱	2224	Gateway IP	172.22.24.254	介面		流量圖細節設定	門檻(kb)	100000			+
交換器	名稱	福環A_1樓_POE	管理 IP	172.22.24.201	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環1F-學務處辦公室-AP	管理 IP	172.22.253.5	上行介面		流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環1F-機房川堂-AP	管理 IP	172.22.253.6	上行介面		流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環1F-教務處辦公室-AP	管理 IP	172.22.253.7	上行介面		流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環B1F-停車場62-AP	管理 IP	172.22.253.62	上行介面		流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環B1F-停車場63-AP	管理 IP	172.22.253.63	上行介面		流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環B1F-停車場64-AP	管理 IP	172.22.253.64	上行介面		流量圖細節設定	門檻(kb)	10000			+
無線基地台	名稱	福環B1F-停車場65-AP	管理 IP	172.22.253.65	上行介面		流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	福環A_2樓_POE	管理 IP	172.22.24.202	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	福環A_5樓_POE	管理 IP	172.22.24.203	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	福環A_8樓_POE	管理 IP	172.22.24.204	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	福環B_2樓_POE	管理 IP	172.22.24.205	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	福環B_5&6樓_POE	管理 IP	172.22.24.206	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	體育館_POE	管理 IP	172.22.24.207	上行介面	225	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	謙禧A_B1樓_POE	管理 IP	172.22.24.209	上行介面	28	流量圖細節設定	門檻(kb)	10000			+
交換器	名稱	謙禧A_B1樓_POE	管理 IP	172.22.24.210	上行介面	225	流量圖細節設定	門檻(kb)	10000			+

設定後資料查詢與監控

拓樸圖

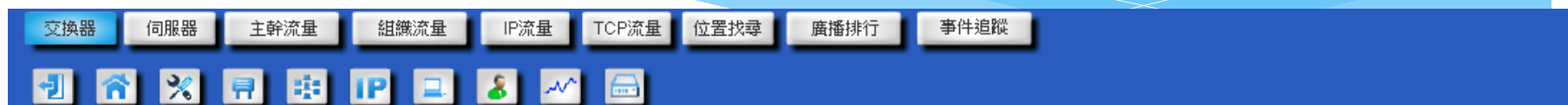
設置完成就可以看到此視窗 可點選資訊視窗看更詳細內容(流量, port接誰等)

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



交換設備狀態

終端在線列表

終端上下線列表

匯出 IP/MAC 總表

交換設備列表

序號	狀態	IP位址	主機名稱	埠	SNMP版本	位置	連結	群組	介面	ARP	MAC	Online	CPU	Memory	OtherC
1.	■	172.22.24.201	福環A_1樓_POE	161	V1		172.22.24.201		inf	ARP	MAC	Online	CPU	RAM	OtherC
2.	■	172.22.24.202	福環A_2樓_POE	161	V1		172.22.24.202		inf	ARP	MAC	Online	CPU	RAM	OtherC
3.	■	172.22.24.203	福環A_5樓_POE	161	V1		172.22.24.203		inf	ARP	MAC	Online	CPU	RAM	OtherC
4.	■	172.22.24.204	福環A_8樓_POE	161	V1		172.22.24.204		inf	ARP	MAC	Online	CPU	RAM	OtherC
5.	■	172.22.24.205	福環B_2樓_POE	161	V1		172.22.24.205		inf	ARP	MAC	Online	CPU	RAM	OtherC
6.	■	172.22.24.206	福環B_5&6樓_POE	161	V1		172.22.24.206		inf	ARP	MAC	Online	CPU	RAM	OtherC
7.	■	172.22.24.207	體育館_POE	161	V1		172.22.24.207		inf	ARP	MAC	Online	CPU	RAM	OtherC
8.	■	172.22.24.208	宿舍大樓_POE	161	V1		172.22.24.208		inf	ARP	MAC	Online	CPU	RAM	OtherC
9.	■	172.22.24.209	CH_B1A	161	V1		172.22.24.209		inf	ARP	MAC	Online	CPU	RAM	OtherC
10.	■	172.22.24.210	CH_B1C	161	V1		172.22.24.210		inf	ARP	MAC	Online	CPU	RAM	OtherC
11.	■	172.22.24.211	CH_1FA	161	V1		172.22.24.211		inf	ARP	MAC	Online	CPU	RAM	OtherC
12.	■	172.22.24.212	CH_1FC	161	V1		172.22.24.212		inf	ARP	MAC	Online	CPU	RAM	OtherC
13.	■	172.22.24.213	CH_3FA	161	V1		172.22.24.213		inf	ARP	MAC	Online	CPU	RAM	OtherC
14.	■	172.22.24.214	CH_3FC	161	V1		172.22.24.214		inf	ARP	MAC	Online	CPU	RAM	OtherC
15.	■	172.22.24.215	CH_4FA	161	V1		172.22.24.215		inf	ARP	MAC	Online	CPU	RAM	OtherC
16.	■	172.22.24.216	CH_4FC	161	V1		172.22.24.216		inf	ARP	MAC	Online	CPU	RAM	OtherC
17.	■	172.22.253.253	Ruckus	161	V2C		https://172.22.253.253		inf	ARP	MAC	Online	CPU	RAM	OtherC
18.	■	172.22.253.254	HP-7506	161	V2C		http://172.22.253.254		inf	ARP	MAC	Online	CPU	RAM	OtherC

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)

ISO insight

版本: v2.7.1.A1.20130905

ISOinsight

系統設定

本機參數

管理員

組織與IP

設備參數

網路拓樸

事件參數

管控策略

語系設定

License管理

網路監視

MAC/IP管理

整合AD認證

流量分析

事件管理

交換器

伺服器

主幹流量

組織流量

IP流量

TCP流量

位置找尋

廣播排行

事件追蹤

主幹流量圖

說明

流量燈號: 以設定的門檻值為判斷依據, 藍 -- 25%以下, 綠 -- 25% ~ 50%, 黃 -- 50% ~ 75%, 橙 -- 75% ~ 100%, 紅 -- 超過門檻值。

網路拓樸列表

HP Core

Router IP: 172.22.253.254

查看設備

VLAN 2224

VLAN IP: 172.22.24.254

福環A_1樓_POE

Switch IP: 172.22.24.201

查看設備

In: 602.7KB

Out: 60.7KB

日流量圖

週流量圖

月流量圖

年流量圖

福環A_2樓_POE

Switch IP: 172.22.24.202

查看設備

In: 1591KB

Out: 184.4KB

日流量圖

週流量圖

月流量圖

年流量圖

福環A_5樓_POE

Switch IP: 172.22.24.203

查看設備

In: 36.2KB

Out: 25.3KB

日流量圖

週流量圖

月流量圖

年流量圖

福環A_8樓_POE

Switch IP: 172.22.24.204

查看設備

In: 39.8KB

Out: 28.9KB

日流量圖

週流量圖

月流量圖

年流量圖

福環B_2樓_POE

Switch IP: 172.22.24.205

查看設備

In: 63.1KB

Out: 30.5KB

日流量圖

週流量圖

月流量圖

年流量圖

福環B_5&6樓_POE

Switch IP: 172.22.24.206

查看設備

In: 104.8KB

Out: 25.1KB

日流量圖

週流量圖

月流量圖

年流量圖

體育館_POE

Switch IP: 172.22.24.207

查看設備

In: 34.6KB

Out: 18.8KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧A_B1樓_POE

Switch IP: 172.22.24.209

查看設備

In: 37.3KB

Out: 21.9KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧C_B1樓_POE

Switch IP: 172.22.24.210

查看設備

In: 0.00KB

Out: 0.00KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧A_1樓_POE

Switch IP: 172.22.24.211

查看設備

In: 124.5KB

Out: 70.0KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧C_1樓_POE

Switch IP: 172.22.24.212

查看設備

In: 649.4KB

Out: 65.7KB

日流量圖

週流量圖

月流量圖

年流量圖

宿舍樓_B1樓_POE

Switch IP: 172.22.24.208

查看設備

In: 1394KB

Out: 114.2KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧A_3樓_POE

Switch IP: 172.22.24.213

查看設備

In: 1736KB

Out: 183.9KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧C_3樓_POE

Switch IP: 172.22.24.214

查看設備

In: 3904KB

Out: 245.6KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧A_4樓_POE

Switch IP: 172.22.24.215

查看設備

In: 1633KB

Out: 137.4KB

日流量圖

週流量圖

月流量圖

年流量圖

謙禧C_4樓_POE

Switch IP: 172.22.24.216

查看設備

In: 7366KB

Out: 655.2KB

日流量圖

週流量圖

月流量圖

年流量圖

VLAN 2980

VLAN IP: 172.22.253.254

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



本: v2.7.1.A1.20130905
ISOinsight

- 系統設定
 - 本機參數
 - 管理員
 - 組織與IP
 - 設備參數
 - 網路拓樸
 - 事件參數
 - 管控策略
 - 語彙設定
 - License管理
- 網路監視
- MAC/IP管理
- 整合AD認證
- 流量分析
- 事件管理

事件觸發

警示設定



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
鎖定事件解鎖後是否重新計算	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.tcmt.edu.tw		
SMTP登入帳號:	sysmang@mail.tcmt.edu.tw		
SMTP登入帳號密碼	*****		
接受通知者的電子郵件地址:	1.	sysmang@mail.tcmt.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

ISO insight

版本: v2.7.1.A.20130905

ISOinsight

系統設定

- 本機參數
- 管理員
- 組織與IP
- 設備參數
- 網路拓撲
- 事件參數
- 管控策略
- 語系設定
- License管理

- 網路監視
- MAC/IP管理
- 整合AD認證
- 流量分析
- 事件管理

6.	啟用設備異常	A43_Cisco_StormControl	Cisco	1	%STORM_CONTROL	disable	disable	0	Y	N	MsgOnly	Cisco交換器發現廣播風暴
7.	啟用設備異常	A45_Cisco_VLAN_MISMATCH	Cisco	1	VLAN_MISMATCH	disable	disable	0	Y	N	MsgOnly	Cisco交換器發現不同VLAN串
8.	啟用設備異常	A46_NBADswitch 3事件	NBADswitch	2	[NS-2980G-26] ARP Spoofing Prevention	disable	disable	0	Y	Y	MsgOnly	NBAD 2980G 事件
9.	啟用設備異常	A47_NBADswitch 3事件	NBADswitch	2	[NS-2980G-26] ARP IPscan Limit Control	disable	disable	0	Y	Y	MsgOnly	NBAD 2980G 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_監控服務異常	NBADmanager	1	log_id=nbad0001,attack_id=10000012	disable	disable	0	Y	Y	MsgOnly	伺服器TCP服務反應超過臨界
12.	啟用Ruckus_AP	AP 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	Y	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秒)	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 阻擋	手動	MAC	120	N	N	MsgOnly	MAC/IP不符合管控策略
19.	啟用地址異常	B18_ARP_Reply 異常	NBADsensor	3	錯誤封包數 增數 > 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	偵測封鎖等待時間 5 分鐘	手動	MAC	10	N	N	MsgOnly	MAC/IP/PORT不符合管控策略
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	NBADanalyzer	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
23.	啟用行為異常	D11_目的埠數分析	NBADanalyzer	1	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
24.	啟用行為異常	D12_目的會談數分析	NBADanalyzer	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
25.	啟用行為異常	D13_超流分析	NBADanalyzer	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_蠕蟲規則分析	NBADanalyzer	1	log_id=nbad0001,attack_id=10000004	手動	Port	1440	N	N	MsgOnly	發現用戶會談行為疑似蠕蟲特
27.	啟用Ruckus_AP	SSID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



版本: v2.7.1.A1.20130905

ISOinsight

- 系統設定
 - 本機參數
 - 管理員
 - 組織與IP
 - 設備參數
 - 網路拓撲
 - 事件參數
 - 管控策略
 - 語系設定
 - License管理
- 網路監視
- MAC/IP管理
- 整合AD認證
- 流量分析
- 事件管理

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

請選擇範圍: 近1小時 或 今天 或 本星期 或 自訂: 2014 / 03 / 26 10 : 49 至 2014 / 03 / 26 11 : 49

事件等級 訊息來源 來源IP 來源MAC 訊息

請輸入條件:

首頁

上頁

下頁

末頁

Goto

 頁

共[8703]項紀錄，搜尋結果共[175]頁，本頁為第[1]頁 [Downl](#)

Syslog列表

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: eventd_to_syslog():User[94:35:0a:b5:c6:65] disconnects from WLAN[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: eventd_to_syslog():User[94:35:0a:b5:c6:65] leave WLAN[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	172.22.253.148			20140326 11:48:52	<3> Mar 26 03:53:14 syslog: lwapp_wtp_snd_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: eventd_to_syslog():User[94:35:0a:b5:c6:65] joins WLAN[TCMT-wlan] from AP[CS-2F-A201@2c:e6:cc:29:42:d0]
5.	info	172.22.253.253			20140326 11:48:52	<134>Mar 26 11:53:00 syslog: eventd_to_syslog():User[98:03:d8:93:00:c0] joins WLAN[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

The screenshot displays a web browser window with two tabs, both showing the URL `172.22.253.252/isoinsight`. The active tab is displaying `172.22.253.252/isoinsight/tbindex.php?authkey=10o9trgpdof3v15mbcf8fev8fojd84`.

The interface features a blue sidebar on the left with the **ToolBoxes** logo and the version `版本: v2.7.1.A1.20130905`. Below the version, the sidebar lists several categories and their sub-items:

- ISOinsight-ToolBoxes
 - DHCP伺服器
 - DHCP(IPv4)
 - DHCP(IPv6)
 - RADIUS伺服器
 - 系統工具箱
 - 重啟/關機** (highlighted)
 - 韌體更新
 - 回復出廠值
 - 常用服務表
 - TFTP暫存檔目錄
 - Script 編輯與派送
 - 下載區
 - SQL-查詢工具
 - 簡訊系統
 - BYOD入網申請維護
 - 拓撲底圖置換

The main content area on the right is titled **關閉/重啟主機** (Shutdown/Restart Host). It contains two sections:

- 說明** (Description): 關閉或重啟本機。 (Shutdown or restart the host.)
- 操作** (Operation): Two buttons labeled **關機** (Shutdown) and **重啟** (Restart).

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

← → ↻ 172.22.253.252/isoinight/tempindex.php?authkey=2o9trgpdof3v15mbcfv8fojd84



版本: v2.7.1.A1.20130905
ISOinsight

- 系統設定
 - 本機參數
 - 管理員
 - 組織與IP
 - 設備參數
 - 網路拓撲
 - 事件參數
 - 管控策略
 - 語系設定
 - License管理
- 網路監視
 - MAC/IP管理
 - 整合AD認證
 - 流量分析
 - 事件管理

網路與介面 系統時間 資料備份 網路服務 系統狀態



資料與備份

儲存

本機組態備份/還原
組態備份 檔案上傳

本機資料儲存期限設定
資料儲存時間為 90 天

遠端備份

硬碟位置	總容量(KB)	已用(KB)	可用(KB)	使用率	狀態
本機	51,606,140	2,198,536	46,786,164	5%	on
遠端	[none]				off,unmount



遠端IP	
遠端目錄	
Login ID	
Password	

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

The screenshot shows a web browser window with two tabs. The active tab is titled '172.22.253.252/isoinsight' and the address bar shows the URL '172.22.253.252/isoinsight/tbindex.php?authkey=11o9trgpdof3v15mbcf8fojd84'. The page has a blue header with the 'ToolBoxes' logo. On the left is a sidebar menu with the following items: '版本: v2.7.1.A1.20130905', 'ISOinsight-ToolBoxes', 'DHCP伺服器' (containing 'DHCP(IPv4)' and 'DHCP(IPv6)'), 'RADIUS伺服器', '系統工具箱' (containing '重啟/關機', '韌體更新' (highlighted in orange), '回復出廠值', '常用服務表', 'TFTP暫存檔目錄', 'Script 編輯與派送', and '下載區'), 'SQL-查詢工具', '簡訊系統', and 'BYOD入網申請維護' (containing '拓樸底圖置換'). The main content area has a blue header with the title '韌體更新'. Below this is a '說明' (Description) section with the text: '更新本機的韌體版本, 修正並新增韌體功能。升級完成, 系統會自動重啟。手動強制重啟可能會造成升級失敗或系統檔案丟失。此外, 不建議遠程升級, 網路傳輸過程有可能造成升級檔案不完整而導致升級失敗。' Below the description is a '操作' (Operation) section. On the right side of the page, it says '目前系統版本為 v2.7.1.A1.20130905' and '檔案上傳' (Upload File).

實機畫面操作 與逐項說明

實機畫面操作後 問題討論

Q & A