



國防大學電算中心

Information Management Center

服務・支援・雲端・網路・整合



區網會議分享報告

報告人：電算中心網路組莊孟翰



大 綱

- 學校簡介。
- 校園網路介紹。
- 工作淺談與網路管理實務。

國防大學電算中心

Information Management Center

服務・支援・雲端・網路・整合





國防大學

National Defense University

學校簡介

率真校區(桃園八德) ★★

軍事學院(戰爭、陸軍、海軍、空軍等學院)

中正嶺校區(桃園大溪) ★

理工學院(國科、電機、電子、資工、機航、
化學材料、環工、動力等科系)

復興崗校區(台北北投) ★

管理學院(法律、財務、運籌、資管、資策等科系)

政戰學院(政治、新聞、應用藝術、社工等科系)

National Defense University

校園公共藝術



校園公共藝術



學校簡介-讀軍事大學的好處

1. 每個月有零用錢，父母不用花錢
2. 洗澡從小時變分鐘
3. 棉被亂七八糟變成豆腐塊
4. 變得有禮貌
5. 燙衣服呱呱叫
6. 打掃、洗碗還會補紗窗
7. 駝背變成挺直
8. 回家覺得菜變好吃
9. 作息正常眼睛都亮了
10. 身體變強壯變健康(定期運動跑步)

校園網路介紹

軍事網路

學術網路

校園網路介紹

軍事網路

- (1)獨立區域網路
- (2)資安管制嚴格
 - a. 網路開通管制
 - b. USB管制
 - c. 資料交換

校園網路介紹

學術網路

- (1) 網路設備電算中心統一納管
- (2) 網管隨時待命
- (3) 資安事件查不完
- (4) 網路大小事找網管

校園網路介紹-學網資安設備

1. 骨幹防火牆(palo alto 5050)

政策規定：只開放80及443 Port

2. 網頁過濾器(WebSense)

(1)禁止網頁(遊戲、賭博、色情、暴力)

(2)上網行為;查看封包(安裝憑證)80、443port

3. 網路流量分析器(Cyberbox)

分析IP行為- 關聯性;橫向感染

校園網路監控系統的選擇

目前市面上有眾多的網路監控系統，如果排除掉須付費的系統外，在免費開放的網路監控系統之中，有Cacti、Nagios及Monit 等系統，而在本校則是選擇導入Cacti這一套網路監控系統。



校園網路監控系統的選擇

Cacti是一套網路監控系統，他最大的優點就是在於Open Source，沒有任何版權受限的問題，也不需要任何License費用，Cacti的特色包含：無限制流量圖形、高可用性資料源，大眾化SNMP Support、帳號管控權限等，並且可以整合包含：Router、Switch、Linux Server、Windows Server等，收集資料涵蓋CPU使用率、RAM使用量、LAN使用量等，在這眾多的優點之下，因此選擇了Cacti 作為校園網路的監控系統。



網路監控系統 安裝準備

安裝Cacti網路監控系統，硬體方面，只需要一台小小的伺服器主機，本次架設採用是IBM 3350 的伺服器主機，軟體方面，採用LINUX CentOS 6作業系統，最後在安裝從Cacti官方網站上免費下載的Cacti監控系統。



網路監控系統 所需安裝套件

要能夠使Cacti網路監控系統運作起來，必須在Linux作業系統上依序安裝Apache網頁伺服器、MySQL資料庫及SNMP服務，然後再進行一些設定的調校與防火牆的規則。

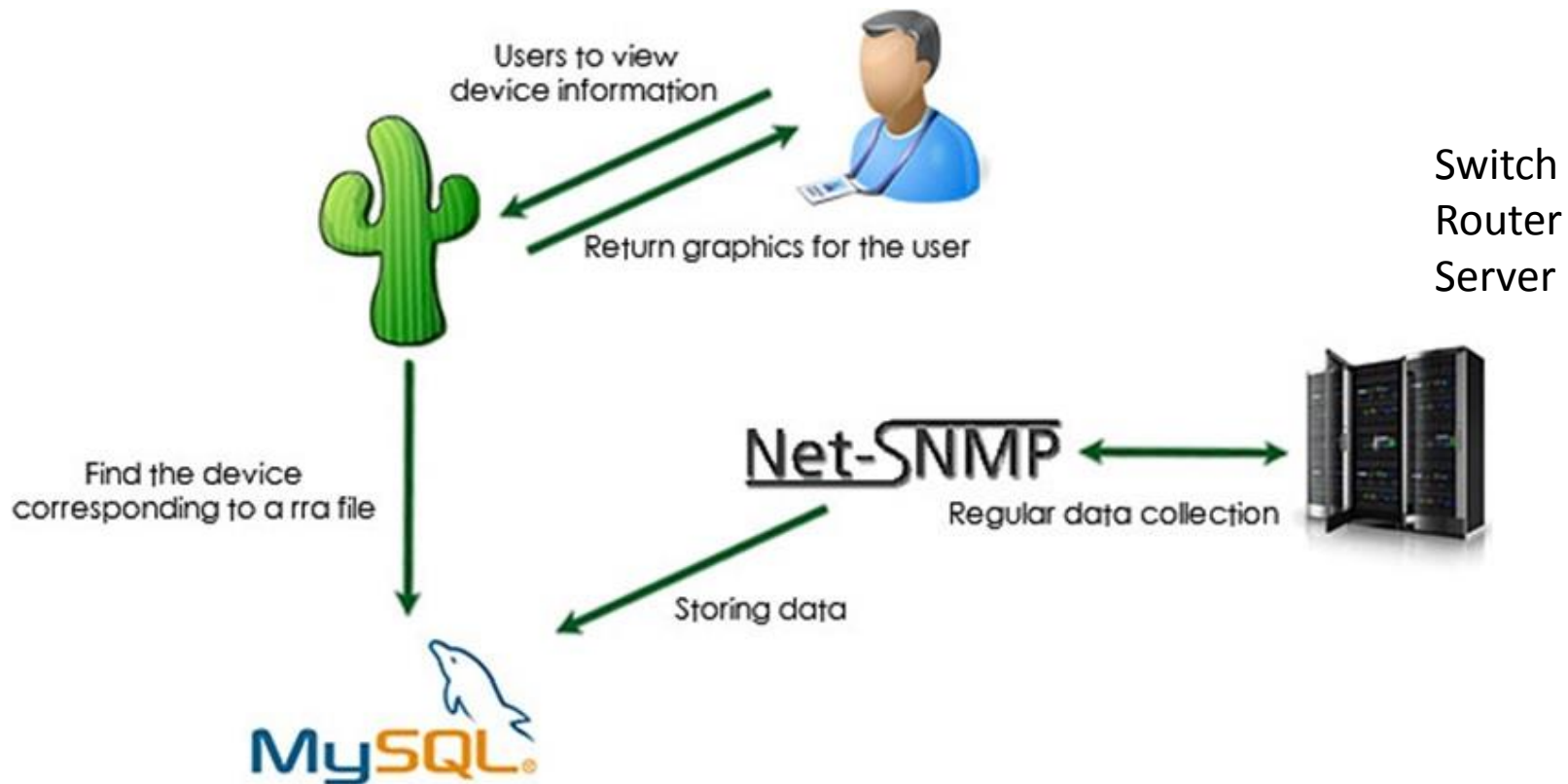
```
yum install mysql* net-snmp* php* freetype-devel libpng-devel libart-lvgl-devel rrdtool* httpd -y
chkconfig snmpd on
chkconfig snmpd --list
snmpwalk -v 1 -c public localhost
iptables -t filter -A INPUT -p udp -dport 161 -h ACCEPT
cd -R cacti-0.8.8a /var/www/html/cacti
*/1 * * * * /usr/bin/php /var/www/html/cacti/poller.php > /dev/null 2>&1
chkconfig mysqld --list
```



Cacti監控系統 運作原理

Cacti是一種運作於伺服器上的網站，其程式碼採用PHP語法內嵌於網頁中，所以管理者在查詢資訊前，所有監控設備的資料透過SNMP協定，存入MySQL資料庫，舉例如Switch可收集單一Port之流量資訊與設備負載，可辨識誰占用最多流量，Router則可收集校園的Routing Table與設備負載，搭配Mac Track模組可解析出該設備之hostname、IP、Mac所有資訊，以上所有資訊最終都是會存入資料庫，當管理者連線至Cacti Web Server 時，就會透過PHP的mysql_connect函式來連線資料庫後將管理者所查詢之條件傳回PHP頁面上。

Cacti監控系統 運作原理



開始導入校園網路設備 監控



User Login

Please enter your Cacti user name and password below:

User Name:

Password:

Login

導入校園網路設備 監控實作

The screenshot displays the Cacti web interface. At the top, there is a navigation bar with tabs for 'console', 'graphs', 'monitor', 'discover', and 'weathermap'. Below this, a header bar shows 'Console' on the left and 'Logged in as admin (Logout)' on the right. The main content area is titled 'You are now logged into Cacti. You can follow these basic steps to get started.' and lists three steps: 'Create devices for network', 'Create graphs for your new devices', and 'View your new graphs'. The first step, 'Create devices for network', is highlighted with a red box, and a red arrow points to it from the right. The left sidebar contains a list of menu items organized into sections: 'Create' (New Graphs), 'Management' (Graph Management, Graph Trees, Data Sources, Devices, Weathermaps), 'Collection Methods' (Data Queries, Data Input Methods), 'Templates' (Graph Templates, Host Templates, Data Templates, Discovery Templates), 'Import/Export' (Import Templates, Export Templates), 'Configuration' (Settings, Plugin Management), and 'Utilities' (System Utilities, User Management, Logout User). The version 'Version 0.8.8a' is displayed in the top right corner.

console graphs monitor discover weathermap

Console Logged in as admin (Logout)

Create

New Graphs

Management

Graph Management

Graph Trees

Data Sources

Devices

Weathermaps

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Data Templates

Discovery Templates

Import/Export

Import Templates

Export Templates

Configuration

Settings

Plugin Management

Utilities

System Utilities

User Management

Logout User

You are now logged into Cacti. You can follow these basic steps to get started.

Create devices for network

- Create graphs for your new devices
- View your new graphs

Version 0.8.8a

導入校園網路設備 監控實作

console

graphs

monitor

discover

weathermap

Console -> Devices -> (Edit)

Logged in as admin (Logout)

Create

New Graphs

Management

Graph Management

Graph Trees

Data Sources

Devices

Weathermaps

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Data Templates

Discovery Templates

Import/Export

Import Templates

Export Templates

Configuration

Settings

Plugin Management

Utilities

System Utilities

User Management

Logout User

Devices [new]

General Host Options

Description

Give this host a meaningful description.

Core switch 6509

Hostname

Fully qualified hostname or IP address for this device.

Cisco 6509-E

Host Template

Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

None

Number of Collection Threads

The number of concurrent threads to use for polling this device. This applies to the Spine poller only.

1 Thread (default)

Disable Host

Check this box to disable all checks for this host.

☐ Disable Host

Monitor Host

Check this box to monitor this host on the Monitor Tab.

☐ Monitor Host

Down Host Message

This is the message that will be displayed when this host is reported as down.

Availability/Reachability Options

Downed Device Detection

The method Cacti will use to determine if a host is available for polling.

SNMP Uptime

NOTE: It is recommended that, at a minimum, SNMP always be selected.

Ping Timeout Value

The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.

400

Ping Retry Count

After an initial failure, the number of ping retries Cacti will attempt before failing.

1

SNMP Options

SNMP Version

Choose the SNMP version for this device.

Version 2

SNMP Community

public

導入校園網路設備 監控實作



The screenshot displays a network monitoring interface. At the top, there is a navigation bar with tabs labeled 'console', 'graphs', 'monitor', 'discover', and 'weathermap'. The 'console' tab is currently selected. Below the navigation bar, the main content area shows a single device entry. On the left side of this entry is a green square icon with a yellow square inside, representing a network device. To the right of the icon, the text 'Core 6509' is displayed. Further to the right, a red text annotation reads '成功加入本校第一台 網路核心交換器'. The left sidebar contains a list of menu items, including 'Create', 'New Graphs', 'Management', 'Graph Management', 'Graph Trees', 'Data Sources', 'Devices', 'Weathermaps', 'Collection Methods', 'Data Queries', 'Data Input Methods', 'Templates', 'Graph Templates', 'Host Templates', 'Data Templates', 'Discovery Templates', 'Import/Export', 'Import Templates', 'Export Templates', 'Configuration', 'Settings', 'Plugin Management', 'Utilities', 'System Utilities', 'User Management', and 'Logout User'. The top right corner of the interface indicates the user is 'Logged in as admin (Logout)'.

console graphs monitor discover weathermap

Console Logged in as admin (Logout)

Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Weathermaps
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Discovery Templates
Import/Export
Import Templates
Export Templates
Configuration
Settings
Plugin Management
Utilities
System Utilities
User Management
Logout User


Core 6509

成功加入本校第一台
網路核心交換器

完成導入校園網路設備監控

console graphs monitor discover weathermap

Console Logged in as admin (Logout)

依序加入本校網路設備

完成加入 126台 網路設備 監控

Core 650 1.CI-A-D-Trendmicro 2.DMZ-2960 SW A-Building(B):2B-37R1 C-Building(B) D-Building

C-Building(A) D-Building -Building(B):3B-29S1 jilding(A):2B-35S1 C-Building(2.DMZ-2960 SW

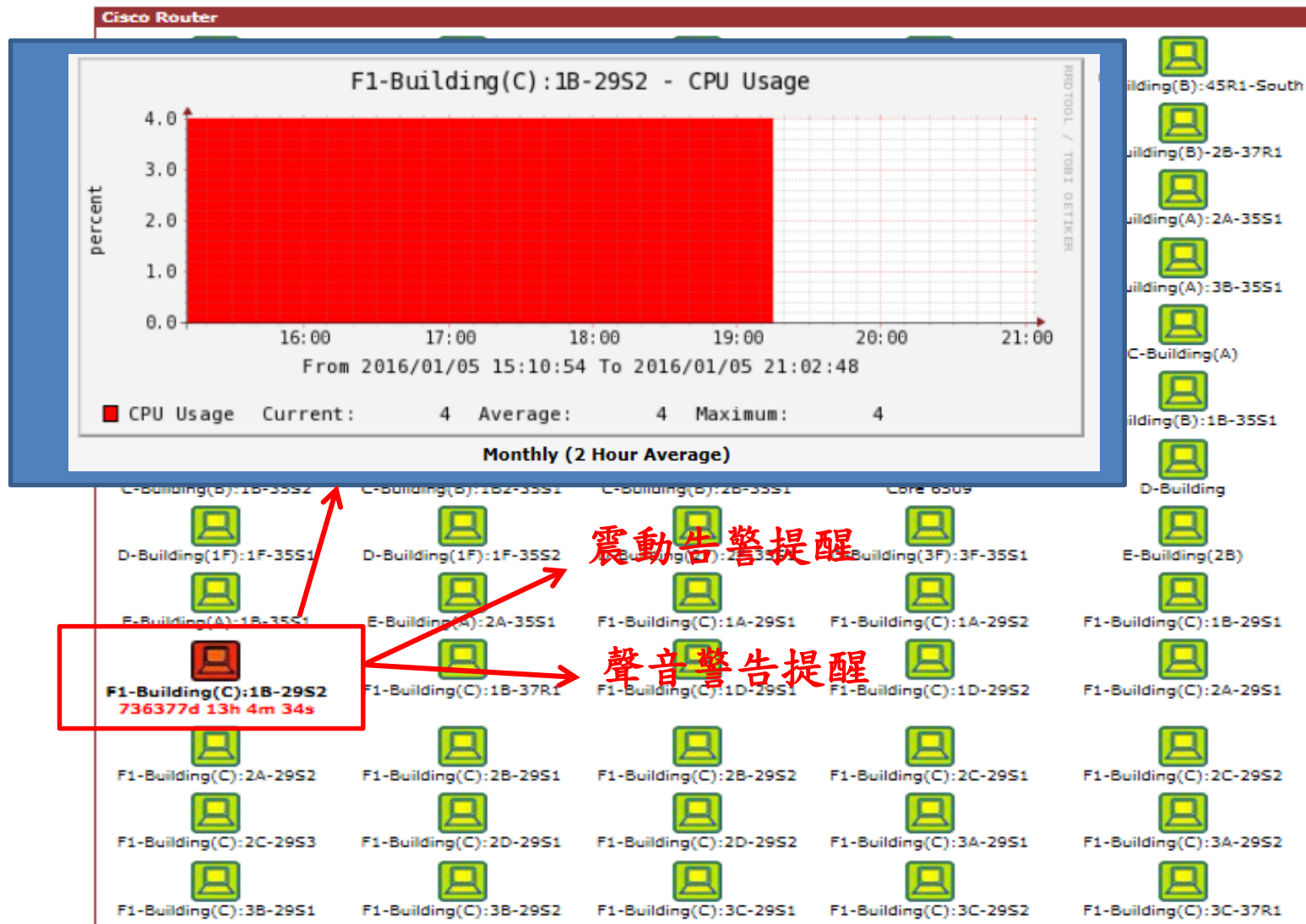
B2-Building(A) Building(B):1B2-35S1 C-Building(A) B2-Building(C):3C-35S1 D-Building C-Building(A)

C-Building(A) .CI-A-D-Trendmicro 2.DMZ-2960 SW C-Building(A) 1.CI-A-D-Trendi 2.DMZ-2960 SW

D-Building C-Building(A) Building(B):1B2-35S1 C-Building(B) C-Building(B) B2-Building(A)

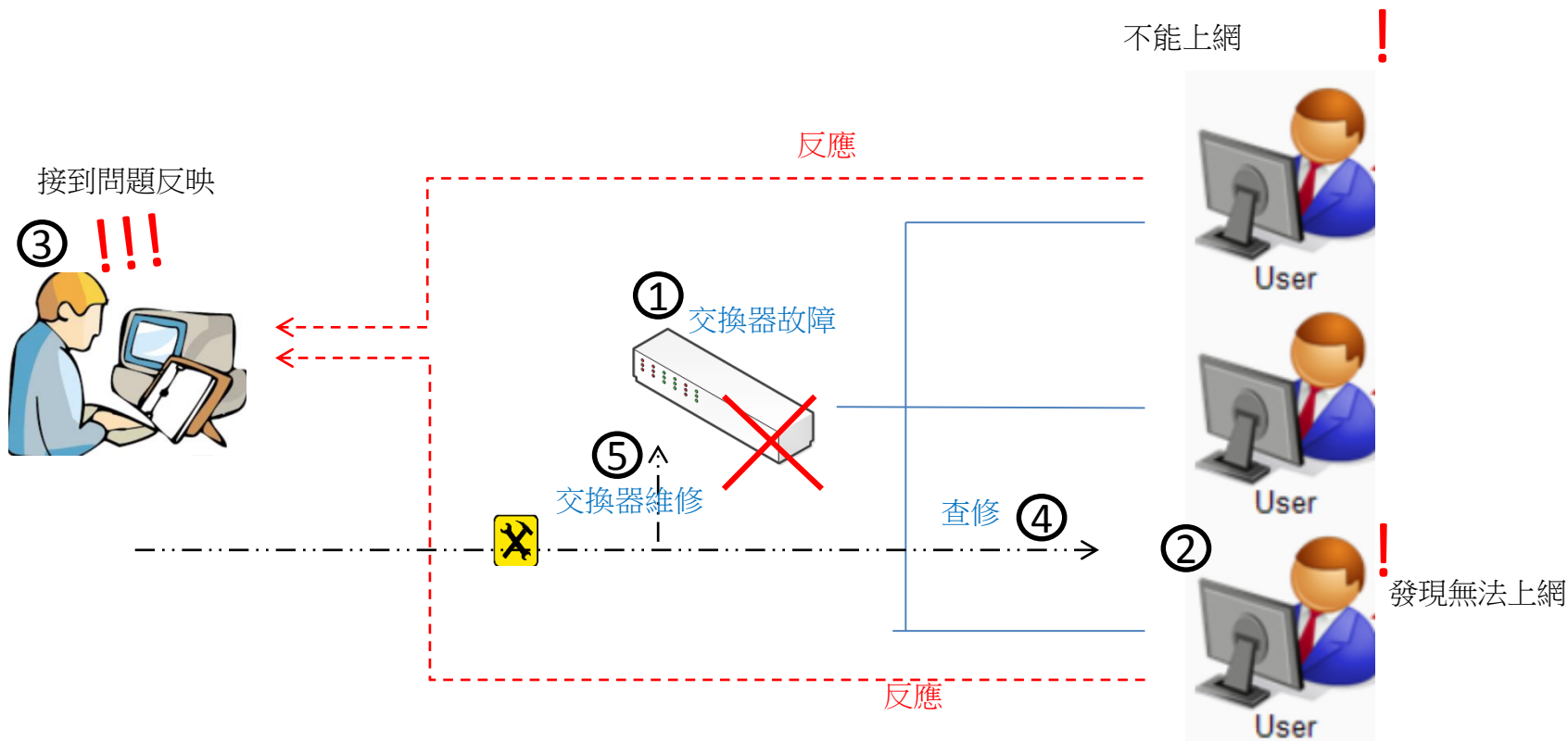
Building(B):1B2-35S1MZ-2960 SW B2-Building(C):3C-35S1 D-Building C-Building(Building(B):1B2-35S1

監控中設備斷線-告警



校園網路監控系統-導入前後比較

校園網路監控系統 導入前維修情形

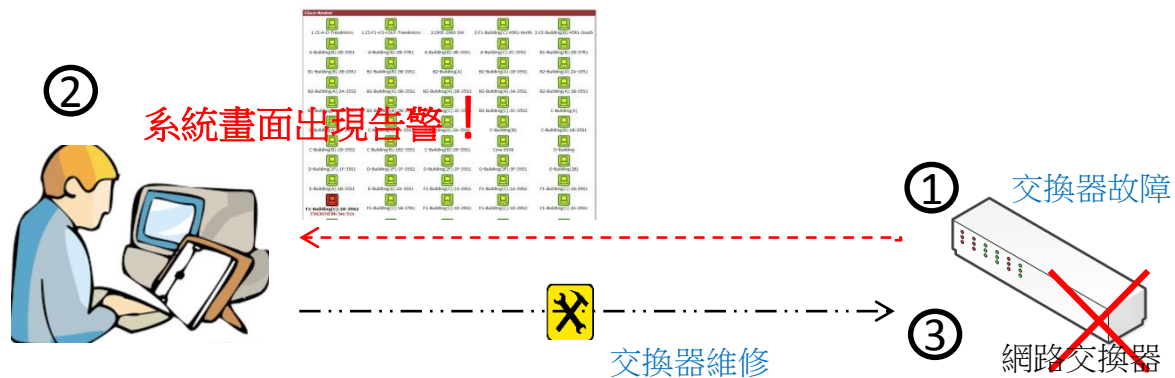


網路設備故障 → 使用者發現網路不通 → 使用者反映問題

網管人員現場查修 → 發現非使用者的問題 → 機房查看發現設備故障

返回調用備援機器 → 再到現場執行維修 → 維修耗時將近一個工作天

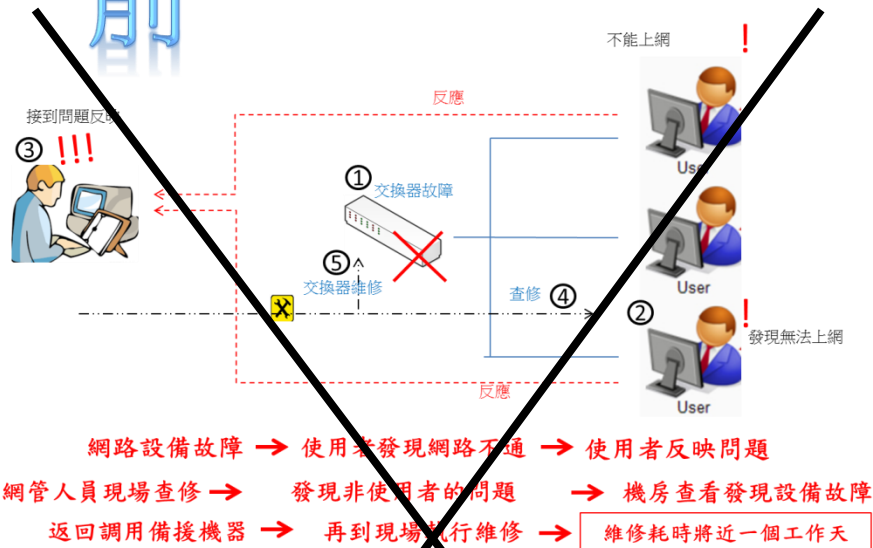
校園網路監控系統 導入後維修情形



網路設備故障 → 監控系統畫面告警 → 網管發現告警
遠端執行無法連線 → 調用備援網路設備 → 前往機房執行維修
→ 維修只需耗時兩個小時

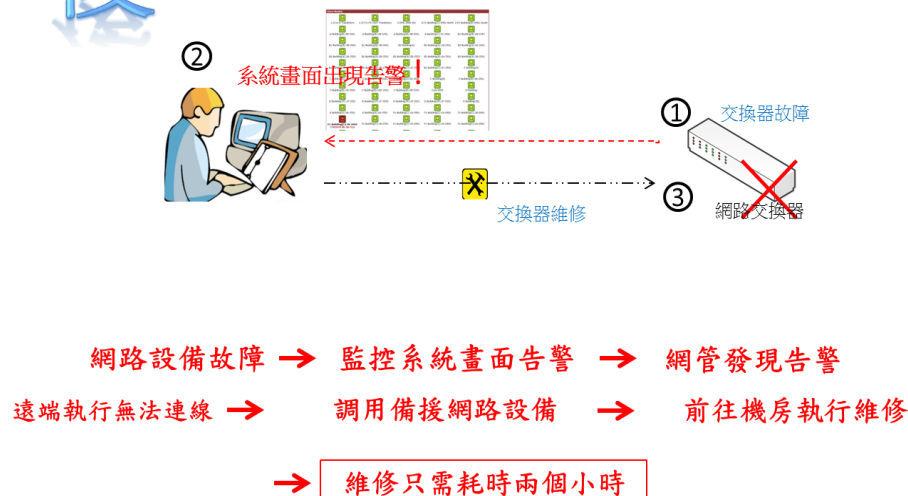
校園網路監控系統 導入前後比較

前



需耗時一個工作天

後



只需耗時兩個小時

校園網路監控系統 導入的結果

@ 大大減省網路查修的時間

@ 網路設備監控一目了然

@ 校園網路流量一把抓

工作淺談-網管人

1. 網路管理(troubleshooting)
2. 資安事件調查(ip查不完)
3. 公文處理(計畫、規定、督導、文來文往)
4. 定期採購與臨時採購(預算時程壓力)
5. 臨時任務

國防大學電算中心

Information Management Center

服務・支援・雲端・網路・整合



報告完畢