交通大學
分享網路管理與資訊安全

2019/07

張瑛杰

暨南大學簡介

暨南大學簡介

暨南大學簡介

暨南大學簡介

自我介紹

張瑛杰

任職於國立暨南國際大學

- 資訊工程學系兼任助理教授
- 計算機與網路中心技術員

學歷

- 國立暨南國際大學國際企業學系博士學位
- 國立暨南國際大學資訊管理學系碩士學位
- 長榮大學企業管理學系學士學位

自民國92年任職於 國立暨南國際大學
擔任台灣高品質學術研究網路(TWAREN) 專任助理
負責 TWAREN GigaPOP 維運業務推動

於民國97年執行台灣學術網路(TANet)
南投區網中心成立與網路管理

多次承接 財團法人台灣網路資訊中心(TWNIC) IPv6
推廣與教育訓練計畫，對象包含政府與學術單位

曾多次接受原廠演講邀約

- 無線網路
- 資訊安全

在 **2017**年 亞太網路資訊中心（ **APNIC**）

Asia-Pacific Network Information Centre

第**44**屆會議上進行發表

長期協助國內不同區網中心與縣網中心
進行教育訓練

在網路與資訊安全領域
有 **14** 年以上的實務經驗

上午場

09:00 ~ 12:00

下午場

13:00 ~ 16:00

伴隨著 TANET / TWAREN
骨幹100G
的新世代發展

校園網路管理
比起十年前更加嚴峻

逐一介紹不同層面的挑戰
以及因應之道

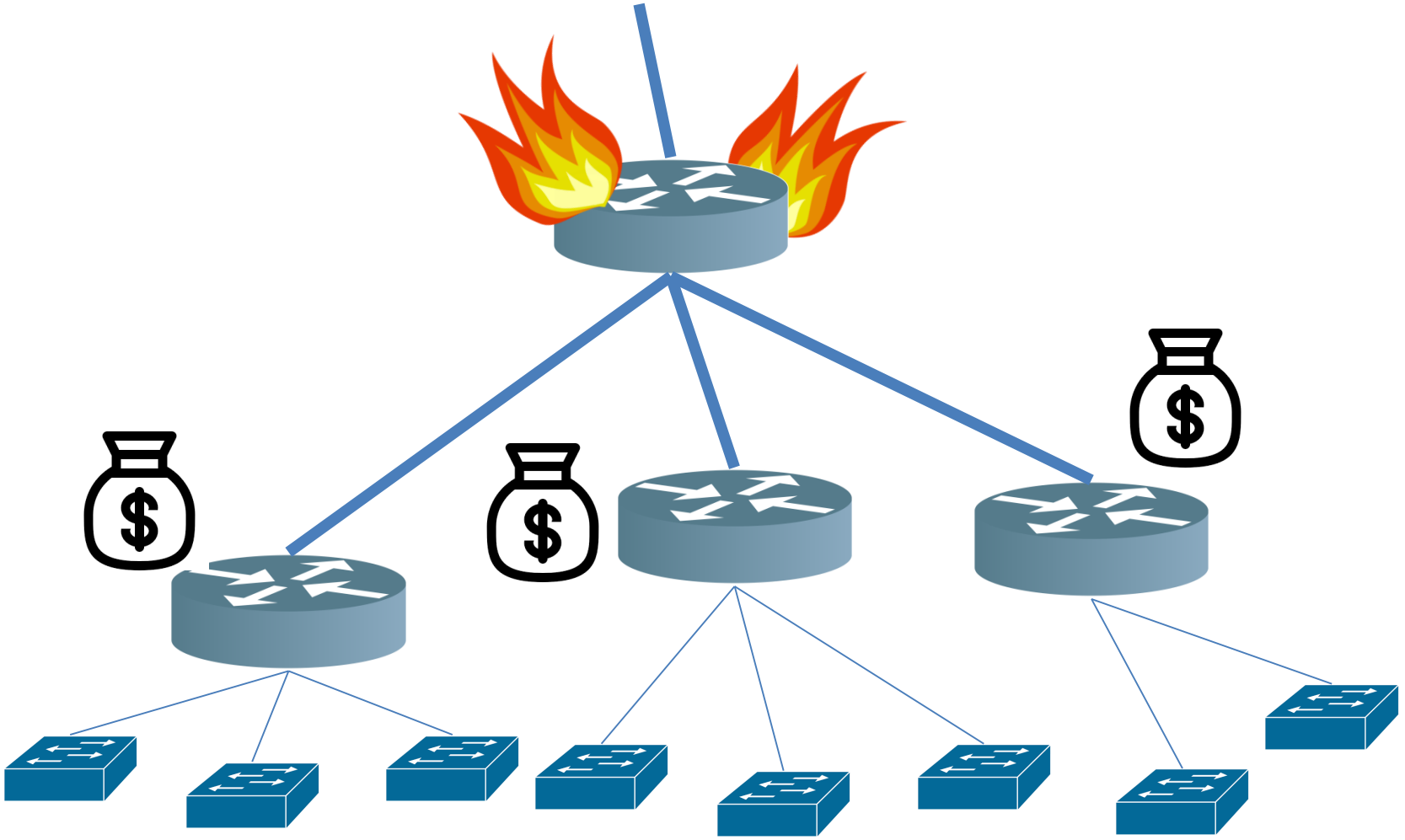
管理五大要訣

- 網路拓樸
- 網段規劃
- 節點資訊
- 設備功能
- 技術資源

核心骨幹的備援機制

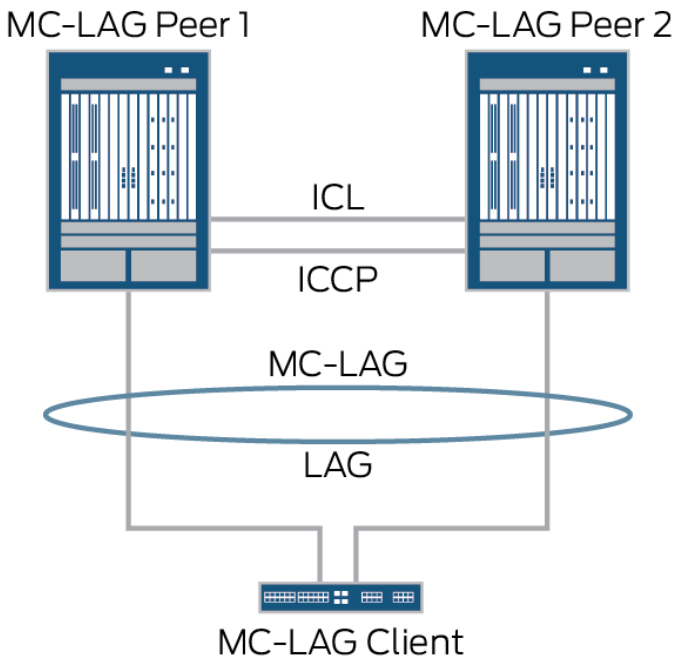
如何挑戰
傳統樹狀拓樸

傳統樹狀拓樸 – 單點故障 / 成本

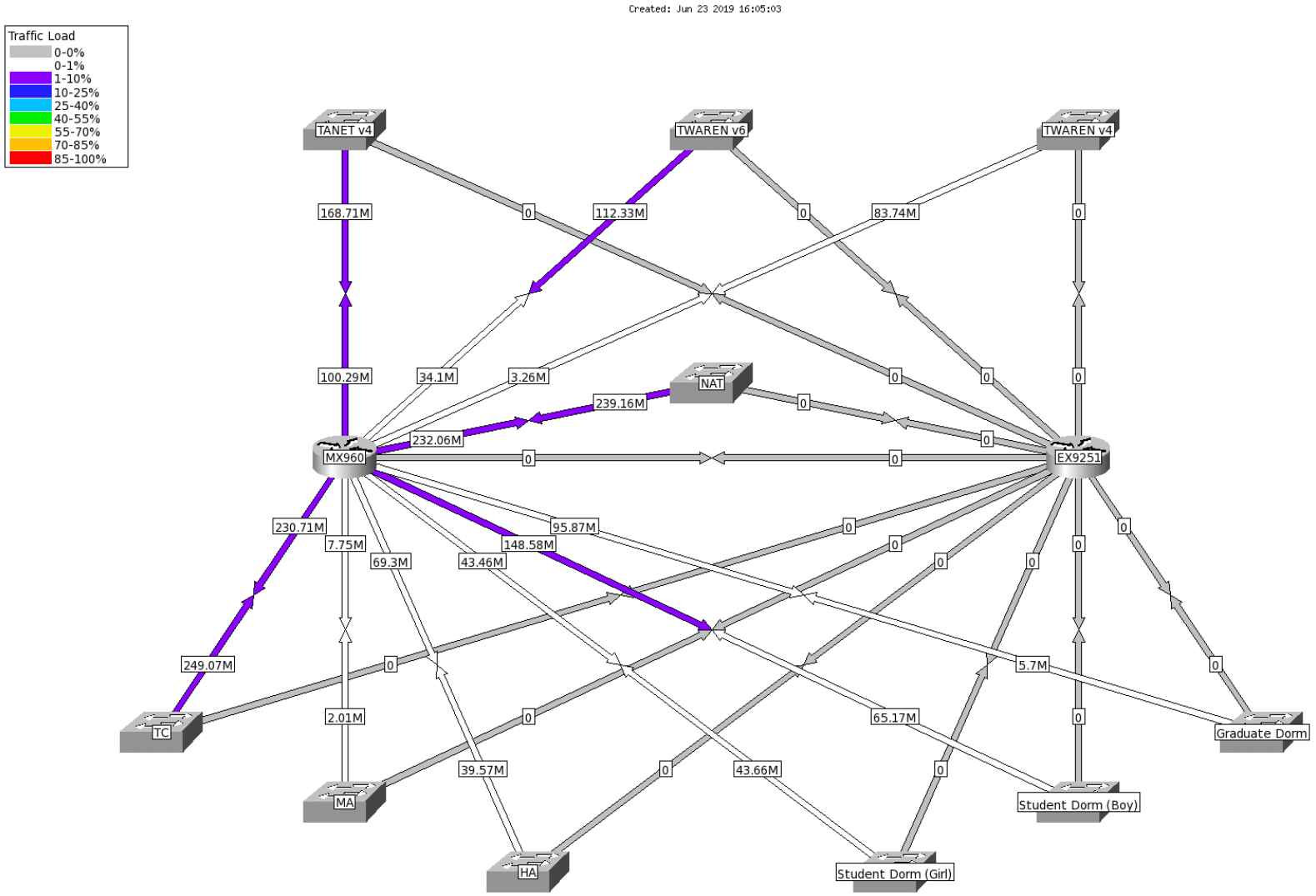


Multi-Chassis Link Aggregation Group (MC-LAG)

Virtual Port-channel (VPC)



繪製簡易學校的網路架構圖



網段規劃

教學大樓

Vlan ID A

163.22.A.0/24

10.10.A.0/24

如果使用者更多怎麼辦?

10.10.B.0/24

10.10.C.0/24

如果網段越多只會...越混亂

建議方案

Vlan ID A

163.22.A.0/24

10.A.0.0/16

2001:e10:6840:A::/64

校園網路節點資訊

- 對照表
  - 牆壁孔
  - Switch port description
  - IP address 與 Switch port
  - MAC 與 Switch port
  - IP address & MAC 與 Switch port 對照表
  - 無線網路 SSID 的編碼

校園內部資安防禦?

內部 – 代表越接近使用者越有效

- 入侵偵測
- 防毒
- 還有....?

17項網管功能測試

管理上須具備的功能

- Syslog
- SNMP
- LOOP Detection
- ARP Spoofing
- Spanning tree
- BPDU
- IP & MAC & PORT
- Multicast
- Netflow / Sflow
- ACL / Filter
- IPv6
- DHCP Snooping
- Port Mirroring
- Storm control
- Commit Confirmed
- Rollback
- 連線方式

SYSLOG

系統提供SYSLOG

包括外送與內存於設備上，並且不因電力中斷而造成設備內存的紀錄消失有利於查修

17項網管功能測試

- Syslog
- SNMP
- LOOP Detection
- ARP Spoofing
- Spanning tree
- BPDU
- IP & MAC & PORT
- Multicast
- Netflow / Sflow
- ACL / Filter
- IPv6
- DHCP Snooping
- Port Mirroring
- Storm control
- Commit Confirmed
- Rollback
- 連線方式

SNMP

具備SNMP v1/v2c/v3

可以透過 polling 的方式取的資訊

MRTG使用須注意超過1G流量務必使用v2c

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

LOOP DETECTION

防止封包一直在迴路中循環而送不出去，導致網路癱瘓，防止最常發生的單點loop

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

ARP SPOOFING

防止GW被假冒

避免使用者被欺騙

綁定 GA MAC

在 UP LINK

限制使用權限

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

SPANNING TREE

同樣是避免迴圈發生

須注意

過大的Domain可能造成效能問題

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

BPDU

防止未經允許下使用者私自接取會發 budp 的 Switch

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

IP & MAC & PORT

允許單一埠執行
IP & MAC 的綁定

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

MULTICAST

運用於電腦教室內的大量派送服務，協助處理以少量頻寬傳送超載的資料，並減輕相關網路設備的負載

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

NETFLOW / SFLOW

提供

Netflow v5/v9

sFlow

流量監控功能

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

ACL / FILTER

提供雙向 ACL
(Access Control List)
封包封鎖之ACL 計數器
封包允許之ACL 計數器

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

IPV6

包括可以透過 IPv6執行的網管方式Syslog、Telnet、SSH、SNMP、NTP & DNS

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

DHCP SNOOPING

確保DHCP Server的回應封包一定會來自合法的DHCP伺服器

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

PORT MIRRORING

可指定port
雙向或單向
進行 mirror

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

STORM CONTROL

避免廣播封包量過大

可以提供告警或封鎖

兩種做法

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

COMMIT CONFIRMED

當修改系統造成本系統失聯時，設定檔須能在指定時間內自動恢復成之前可連線狀態之功能，可節省設定錯誤造成斷線時必須至現場處理的時間

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

ROLLBACK

系統提供多組以時間排序的設定檔儲存，可選擇任一設定檔進行還原，還原過程中網路不中斷

17項網管功能測試

Syslog
SNMP
LOOP Detection
ARP Spoofing
Spanning tree
BPDU
IP & MAC & PORT
Multicast
Netflow / Sflow
ACL / Filter
IPv6
DHCP Snooping
Port Mirroring
Storm control
Commit Confirmed
Rollback
連線方式

連線方式

Console Port、Telnet、SSH及HTTP/HTTPS等方式均可進行網管及參數設定與執行系統軟體更新

17項網管功能測試

12項參數設定

該如何確認有哪些參數

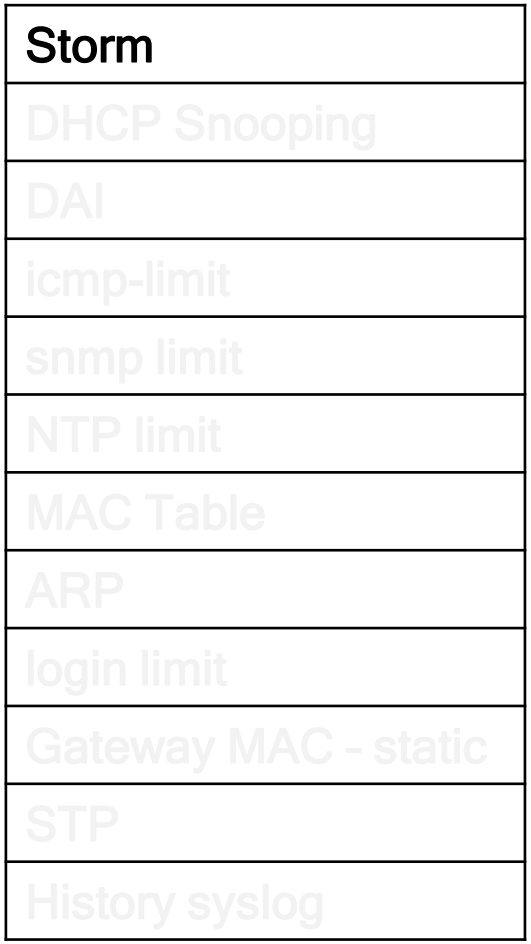
Broadcast

Multicast

Unknown-unicast

Bandwith / Count

STORM



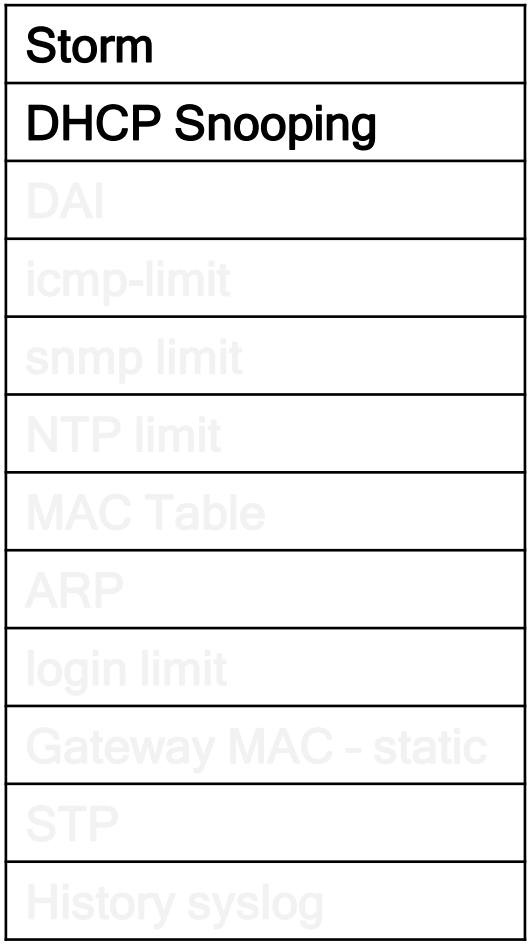
12項參數設定

Trust

un-trust

rate limit

DHCP SNOOPING



12項參數設定

Dynamic ARP inspection

DAI

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC - static
STP
History syslog

12項參數設定

避免跨網段大量掃 IP address

ICMP-LIMIT

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC - static
STP
History syslog

12項參數設定

限制可存取的來源

SNMP LIMIT

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC – static
STP
History syslog

12項參數設定

避免 NTP 放大攻擊

NTP LIMIT

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC - static
STP
History syslog

12項參數設定

限制每一個 port 的 MAC count 以及 MAC table 暫存的 time

MAC TABLE

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC - static
STP
History syslog

12項參數設定

限制同網段廣播封包量以及 Router 上 ARP 暫存的 time

ARP

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC – static
STP
History syslog

12項參數設定

ssh

https

telnet

http

LOGIN LIMIT

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC – static
STP
History syslog

12項參數設定

避免惡意搶奪 Gateway

GATEWAY MAC STATIC

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC - static
STP
History syslog

12項參數設定

避免太大的domain

STP

Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC – static
STP
History syslog

12項參數設定

紀錄資訊是否足以提供判斷

HISTORY SYSLOG

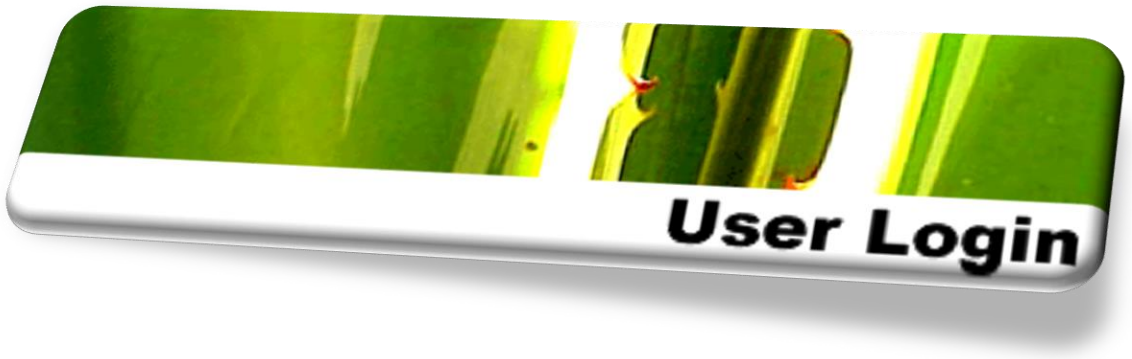
Storm
DHCP Snooping
DAI
icmp-limit
snmp limit
NTP limit
MAC Table
ARP
login limit
Gateway MAC - static
STP
History syslog

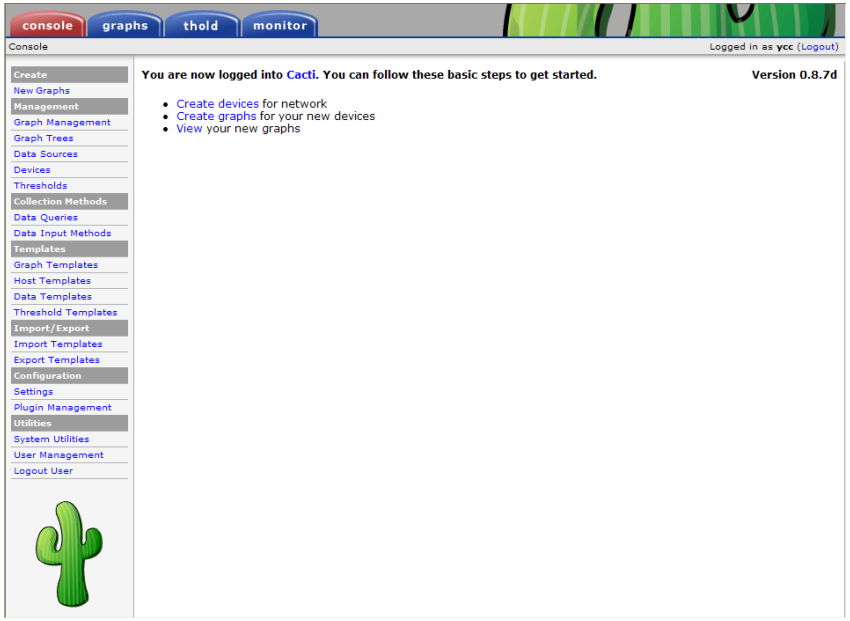
12項參數設定

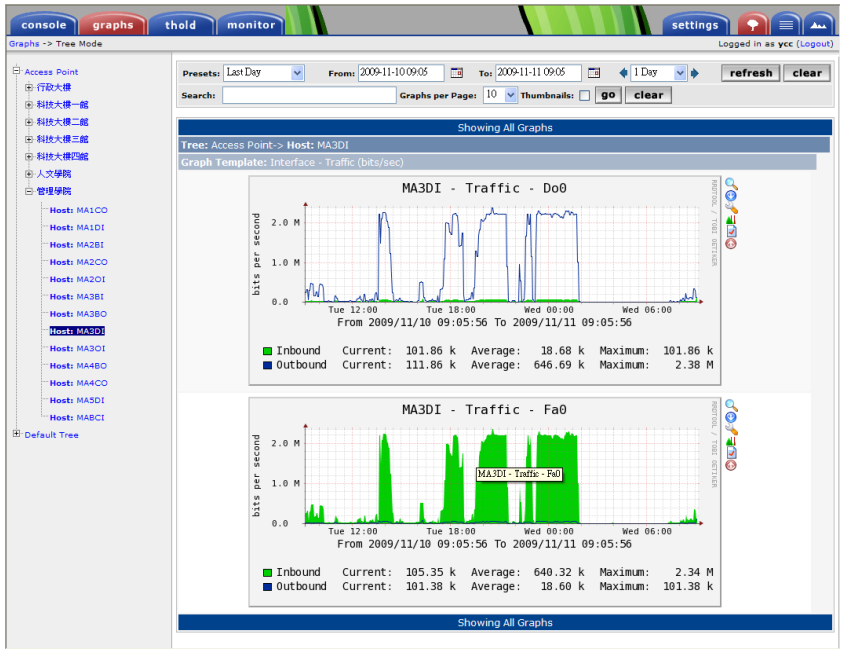
技術支援

- 各校使用經驗交流
- **SOP** 是否出充足
- 廠商的配合程度
- 原廠的支援程度

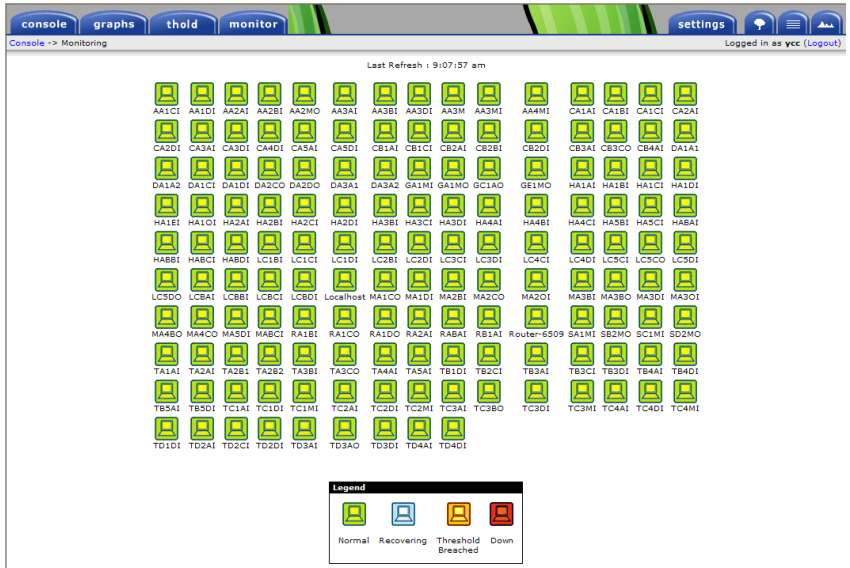
Cacti
網管軟體




console
graphs
thold
monitor
Console
Logged in as ycc (Logout)
Create
New Graphs
Management
Graph Management
Graph Trees
Data Sources
Devices
Thresholds
Collection Methods
Data Queries
Data Input Methods
Templates
Graph Templates
Host Templates
Data Templates
Threshold 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.
Version 0.8.7d
Create devices for network
Create graphs for your new devices
View your new graphs


console
graphs
thold
monitor
settings
Graphs -> Tree Mode
Logged in as ycc (Logout)
Access Point
行政大樓
科技大樓一館
科技大樓二館
科技大樓三館
科技大樓四館
人文學院
管理學院
Host: MA1CO
Host: MA1DI
Host: MA2BI
Host: MA2CO
Host: MA2OI
Host: MA3BI
Host: MA3BO
Host: MA3DI
Host: MA3OI
Host: MA4BO
Host: MA4CO
Host: MA5DI
Host: MABCI
Default Tree
Presets: Last Day
From: 2009-11-10 09:05
To: 2009-11-11 09:05
1 Day
refresh
clear
Search:
Graphs per Page: 10
Thumbnails:
go
clear
Showing All Graphs
Tree: Access Point-> Host: MA3DI
Graph Template: Interface - Traffic (bits/sec)
MA3DI - Traffic - Do0
bits per second
2.0 M
1.0 M
0.0
Tue 12:00
Tue 18:00
Wed 00:00
Wed 06:00
From 2009/11/10 09:05:56 To 2009/11/11 09:05:56
Inbound Current: 101.86 k Average: 18.68 k Maximum: 101.86 k
Outbound Current: 111.86 k Average: 646.69 k Maximum: 2.38 M
MA3DI - Traffic - Fa0
MA3DI - Traffic - Fa0
From 2009/11/10 09:05:56 To 2009/11/11 09:05:56
Inbound Current: 105.35 k Average: 640.32 k Maximum: 2.34 M
Outbound Current: 101.38 k Average: 18.60 k Maximum: 101.38 k
Showing All Graphs


console
graphs
thold
monitor
Console -> Devices
Logged in as ycc (Logout)
Devices
Add
Type: Any
Status: Enabled
Search:
Rows per Page: 30
go
clear
<< Previous
Showing Rows 1 to 30 of 146 [1,2,3,4,5]
Next >>
Description** ID Graphs Data Sources Status Event Count Hostname Current (ms) Average (ms) Availability
AA1CI 114 2 2 Up 0 163.22.9.231 7.31 10.56 98.85
AA1DI 113 2 2 Up 0 163.22.9.230 7.15 11.38 98.89
AA2AI 115 2 2 Up 0 10.10.62.235 2.4 2.56 83.35
AA2BI 116 2 2 Up 0 10.10.62.236 2.43 2.61 99.46
AA2MO 117 2 2 Up 0 10.10.62.232 2.5 2.72 99.46
AA3AI 123 2 2 Up 0 10.10.62.230 2.4 2.56 99.46
AA3BI 122 2 2 Up 0 10.10.62.234 2.36 2.53 99.46
AA3CI 120 1 1 Up 0 163.22.9.234 90.24 51.96 95.96
AA3DI 118 2 2 Up 0 163.22.9.232 4.2 10.74 99.31
AA3M 121 2 2 Up 0 10.10.62.233 2.34 2.57 99.46
AA3MI 119 1 1 Up 0 163.22.9.233 86.13 51.89 99.27
AA4MI 124 2 2 Up 0 163.22.9.235 5.45 10.71 99.21
CA1AI 95 2 2 Up 0 10.10.8.221 23.94 8.26 99.13
CA1BI 96 2 2 Up 0 163.22.8.237 9.8 10.95 93.26
CA1CI 97 2 2 Up 0 10.10.8.222 7.36 7.94 99.16
CA2AI 98 2 2 Up 0 10.10.8.223 7.67 7.94 99.15
CA2DI 99 2 2 Up 0 10.10.8.224 7.97 8.38 99.16
CA3AI 100 2 2 Up 0 10.10.8.225 7.28 8.33 99.16
CA3DI 101 2 2 Up 0 10.10.8.226 7.49 8.27 99.16
CA4DI 102 2 2 Up 0 10.10.8.228 7.32 8 99.15
CA5AI 103 2 2 Up 0 10.10.8.229 10.56 7.98 99.16
CA5DI 104 2 2 Up 0 10.10.8.230 24.43 8.06 99.14
CB1AI 105 2 2 Up 0 10.10.8.231 7.75 8.1 99.19
CB1CI 106 2 2 Up 0 163.22.8.238 6.5 10.93 99.41
CB2AI 107 2 2 Up 0 10.10.8.232 7.85 8.23 99.18
CB2BI 108 2 2 Up 0 10.10.8.233 7.31 7.94 96.33
CB2DI 109 2 2 Up 0 10.10.8.234 2.74 2.66 99.43
CB3AI 110 2 2 Up 0 10.10.8.235 7.38 8.42 99.19
CB3CO 111 2 2 Up 0 10.10.8.236 2.52 2.7 99.43
CB4AI 112 2 2 Up 0 10.10.8.237 7.9 7.98 98.36
<< Previous
Showing Rows 1 to 30 of 146 [1,2,3,4,5]
Next >>


console
graphs
thold
monitor
settings
Console -> Monitoring
Logged in as ycc (Logout)
Last Refresh : 9:07:57 am
Legend
Normal
Recovering
Threshold Breached
Down

IPv4/IPv6 Dual Stack模式下
對資安防護及區域聯防服務推動
的衝擊與影響以及新挑戰

運用SDN技術
解決臺灣學術網路(TANet)
校內資訊安全管理之困境

大綱

臺灣學術網路(TANet)

為了落實網路安全管理

在網路骨幹建構 整 偵測 與 通報 機制

大綱

因為資安政策
各校自主規劃資安防禦設備

大多是將IPS或IDS建置在校園出口

這和 TANet 資訊安全架構有重疊之處

大綱

國中小、高中職

在校園內網 的資訊安全管理

明顯地表現較薄弱

大部分

將資安設備取代核心路由器

在收納層建置小型的資安設備

大綱

當內網大量傳輸

很容易造成單一節點 資安設備 效能不足

原因在受限於資安設備的效能

隨著使用頻寬的提升

變成一個難以解決的問題

希望能分享運用 SDN概念

提出的管理架構

面對頻寬持續增加時的資安挑戰

臺灣學術網路

(Taiwan Academic Network, TANet)

臺灣各級學校網路及資訊教育之平台

臺灣學術網路

教育部及幾個主要國立大學
於民國79年7月起所共同建立的一個全國性
教學研究網路

其主要目的是支援
全國各級學校及研究機構之教學研究活動
促進資源分享與合作

臺灣學術網路

TANet 骨幹網路

- 骨幹網路
- 區域網路中心
- 縣市教育網路中心

TANet 存取網路

- 大專校院
- 高中職校
- 國中小學

教育學術網百G 數位學校創第E

- 教育部
- 中央研究院
- 科技部國家實驗研究院

規劃推動三年期計畫

教育學術研究骨幹網路頻寬效能提升計畫 - 100G骨幹網路

教育學術網百G 數位學校創第E

教育學術網百G 數位學校創第E

105年4月26日開始試營運

建置臺灣高品質、高頻寬學術網路骨幹

國內學研單位教學、研究、實驗

共用的網路平臺，增加雲端服務效能

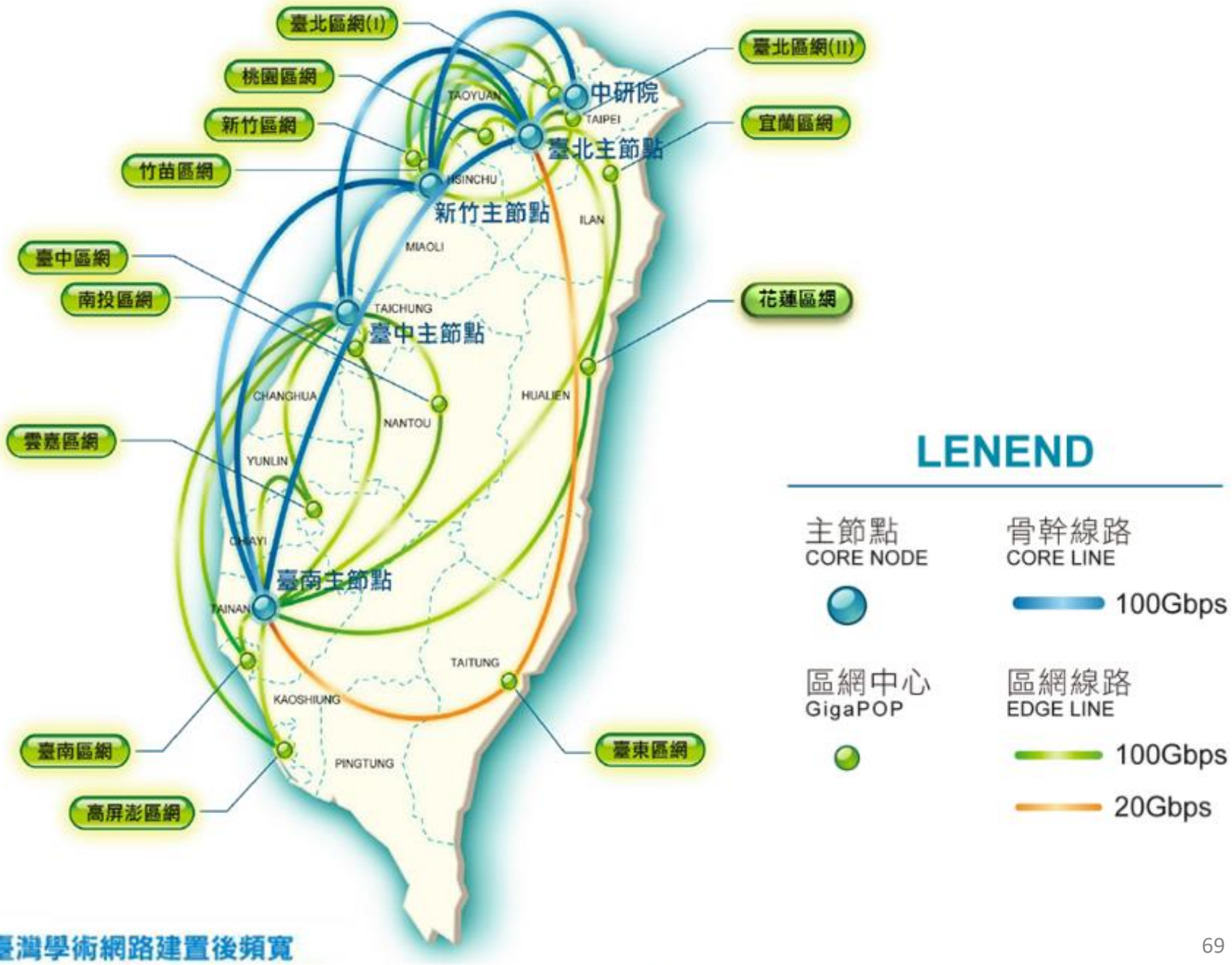
教育學術網百G 數位學校創第E

提供公開透明的網路速度及品質資訊

建構以臺灣為中心
連接亞太、歐美，與全世界接軌的
學術研究網路

記者會現場


教育部
中央研究院
ACADEMIA SINICA
國家高速網路與計算中心
推動高品質．高頻寬臺灣100G學術網路
教育學術網百G 數位校園創第E
主辦單位：教育部．中央研究院．國家實驗研究院國家高速網路與計算中心
協辦單位：各區域網路中心
台北
新竹
台中
TANet
100G
100G



臺灣學術網路建置後頻寬

學術網路資訊安全通報機制

為了落實網路安全管理
在網路骨幹建構完整
偵測與通報機制

資安通報 重要單位

- 台灣學術網路危機處理中心

TANet Computer Emergency Response Team

- 學術資訊安全維運中心

Academic Security Opertion Center

- 區網中心

GigaPOP

當頻寬不斷增加 1G / 10G / 40G / 100G

既有設備依舊正常提供服務
但問題是... 這些設備都只 1G Port 可以進行介接
例如：Firewall、IPS 、IDS

常聽到的解決方法

購買更昂貴的資安設備 10G / 40G

10G / 40G / 100G 的資訊安全設備

在建置成本上都會高於 Router 或 Switch

甚至是倍數成長

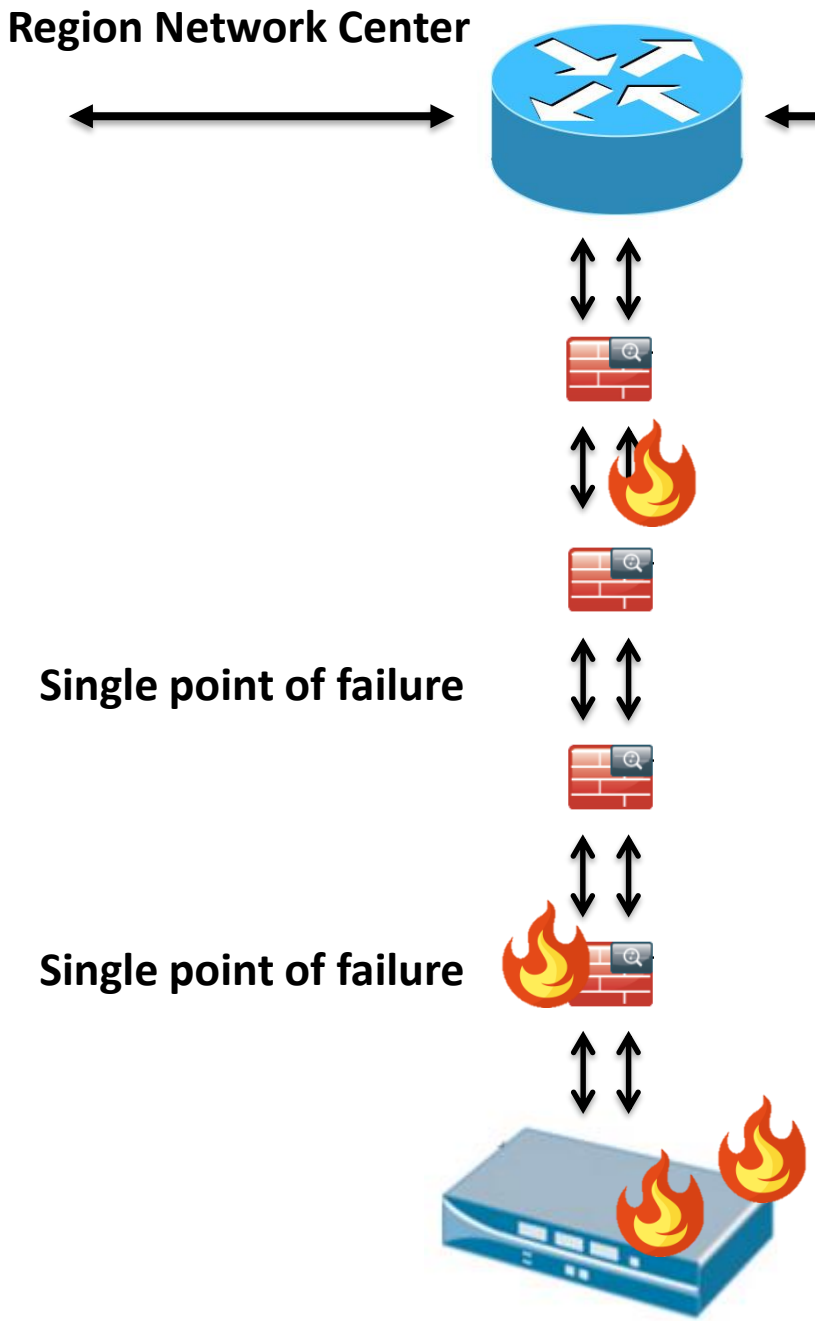
這是一個需要被討論的問題!!!

討論項目

1. SDN-based security supporting infrastructure(I)
   Network and Service bypass

2. SDN-based security supporting infrastructure(2)
   Netflow generation

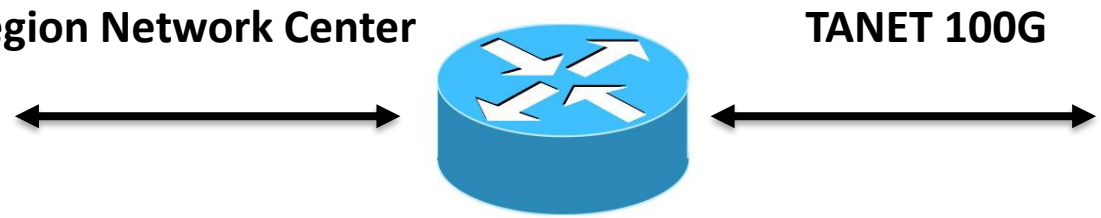
Previous Topology



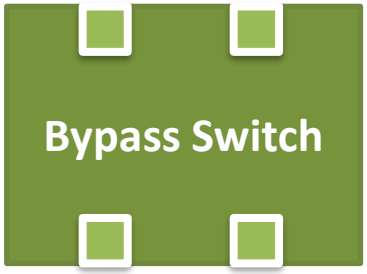
Pitfalls

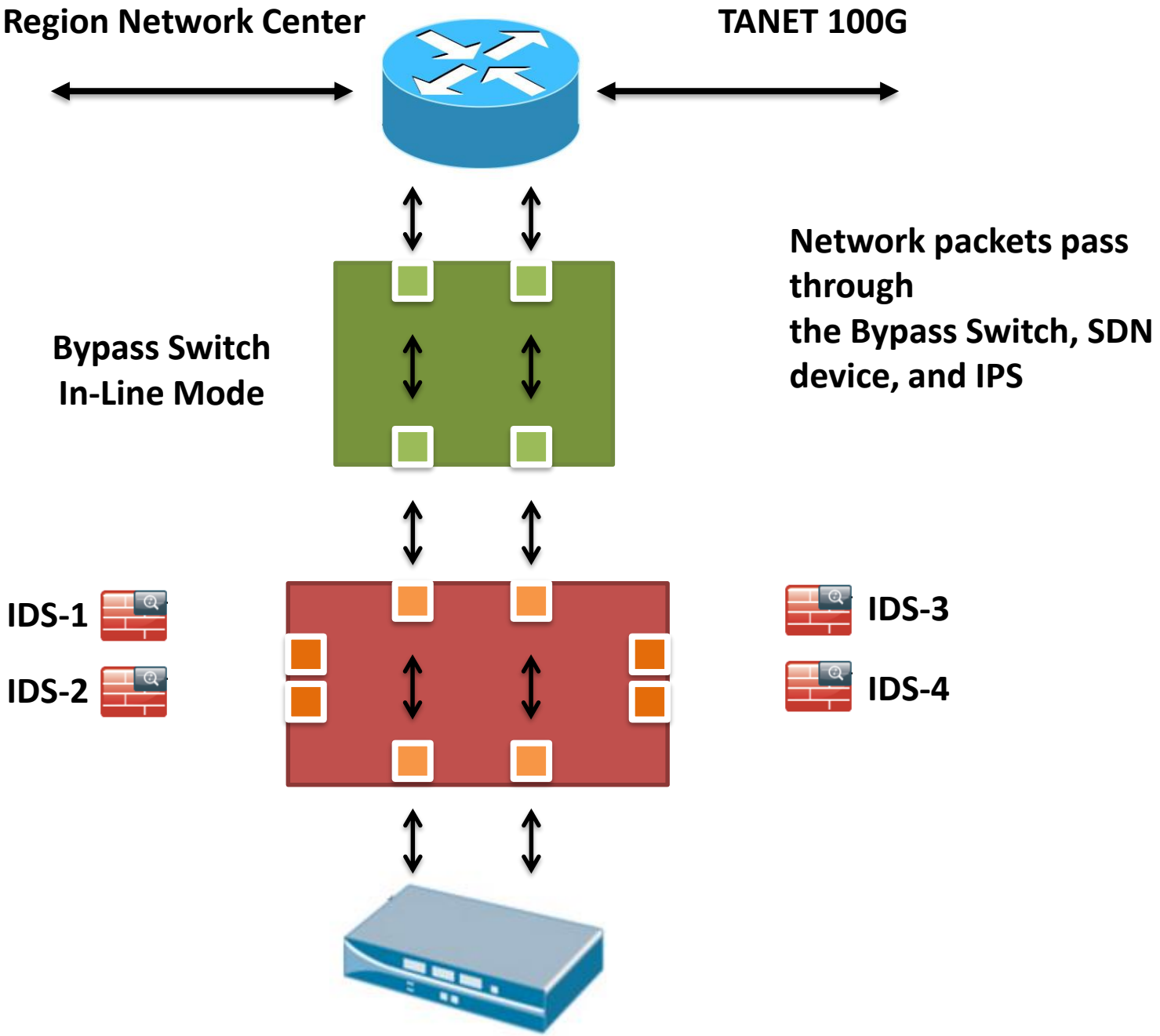
- Devices out of service
- Mini-gbic failure
- Cable / Fiber failure
- Failed configuring

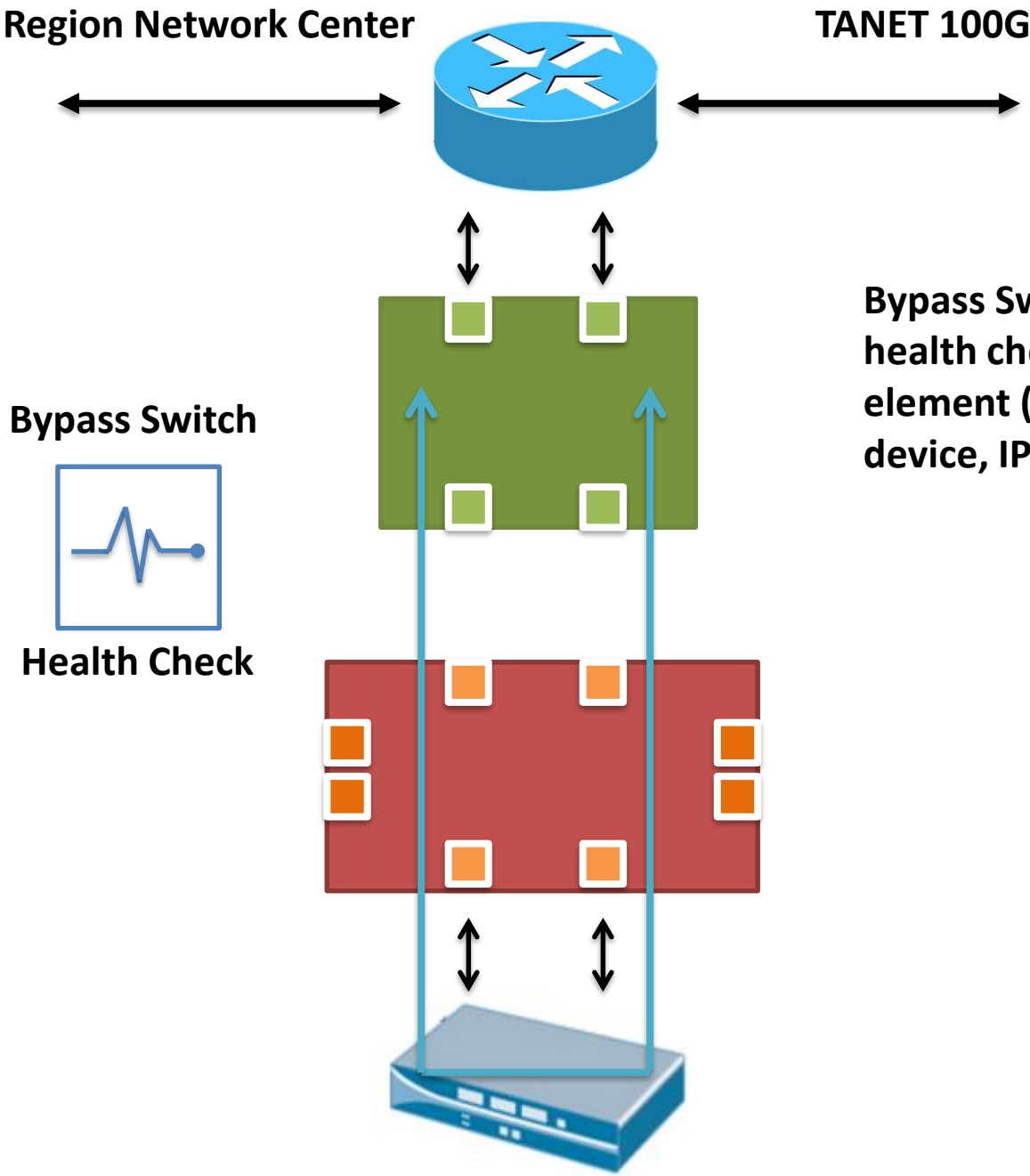
New Topology



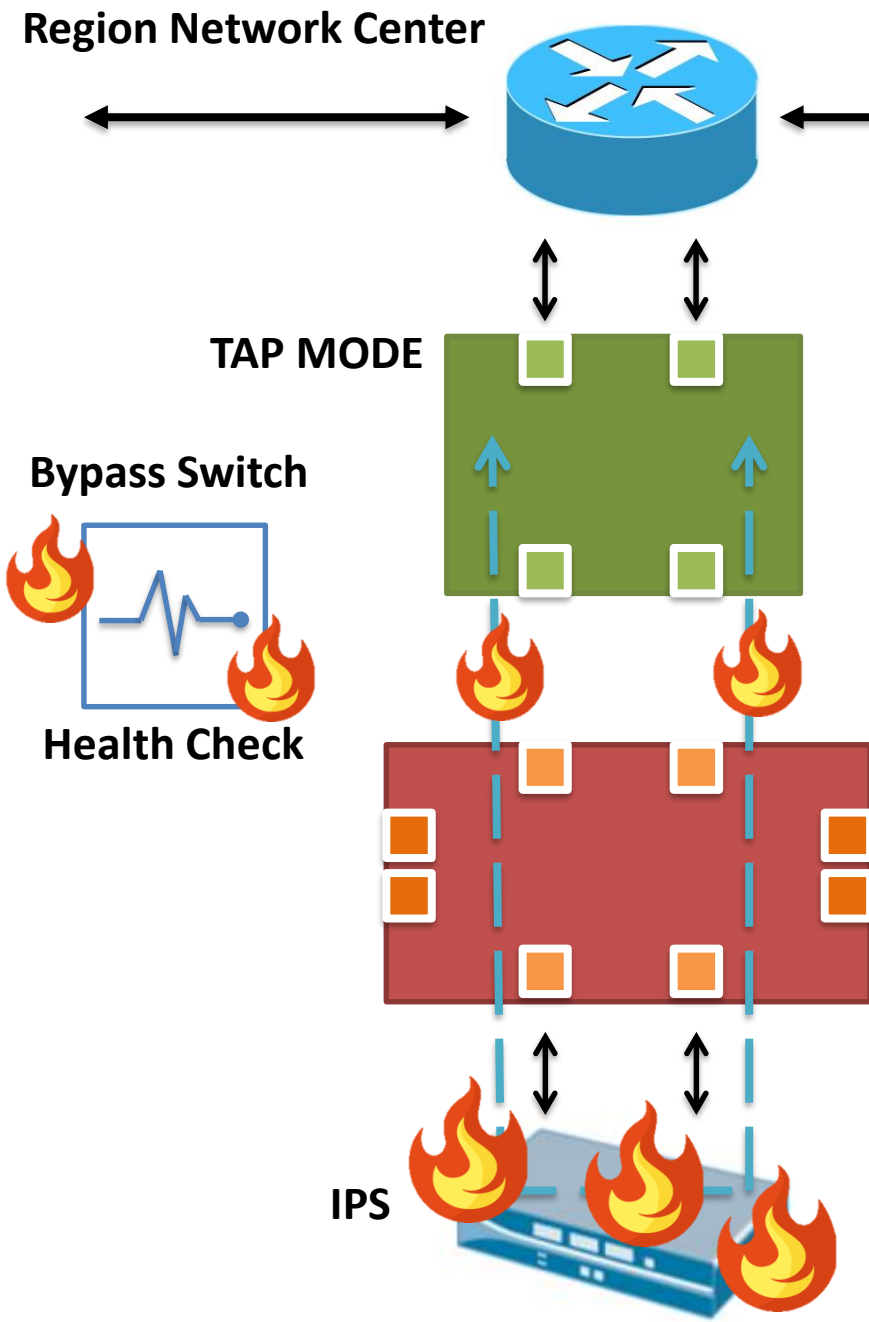
Security Supporting Mechanism:
- Bypass switch
- Proprietary SDN device(L2-L7 support)




Region Network Center
TANET 100G
Bypass Switch
In-Line Mode
Network packets pass
through
the Bypass Switch, SDN
device, and IPS
IDS-1
IDS-2
IDS-3
IDS-4

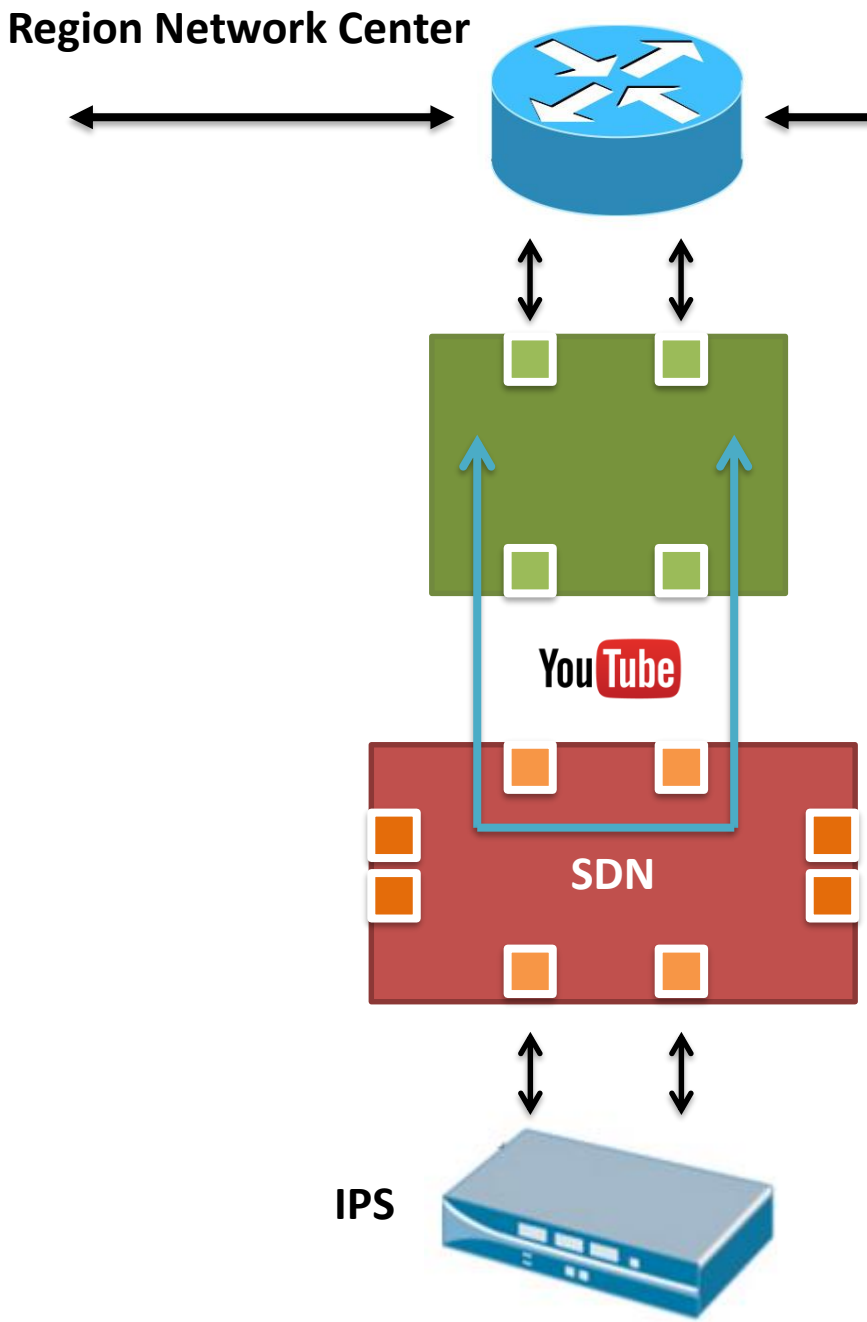


Bypass Switch should provide health check in case any element (including itself, SDN device, IPS) malfunctions.



When some troubles happen…

Health Check packets are lost or delayed a lot(high latency)

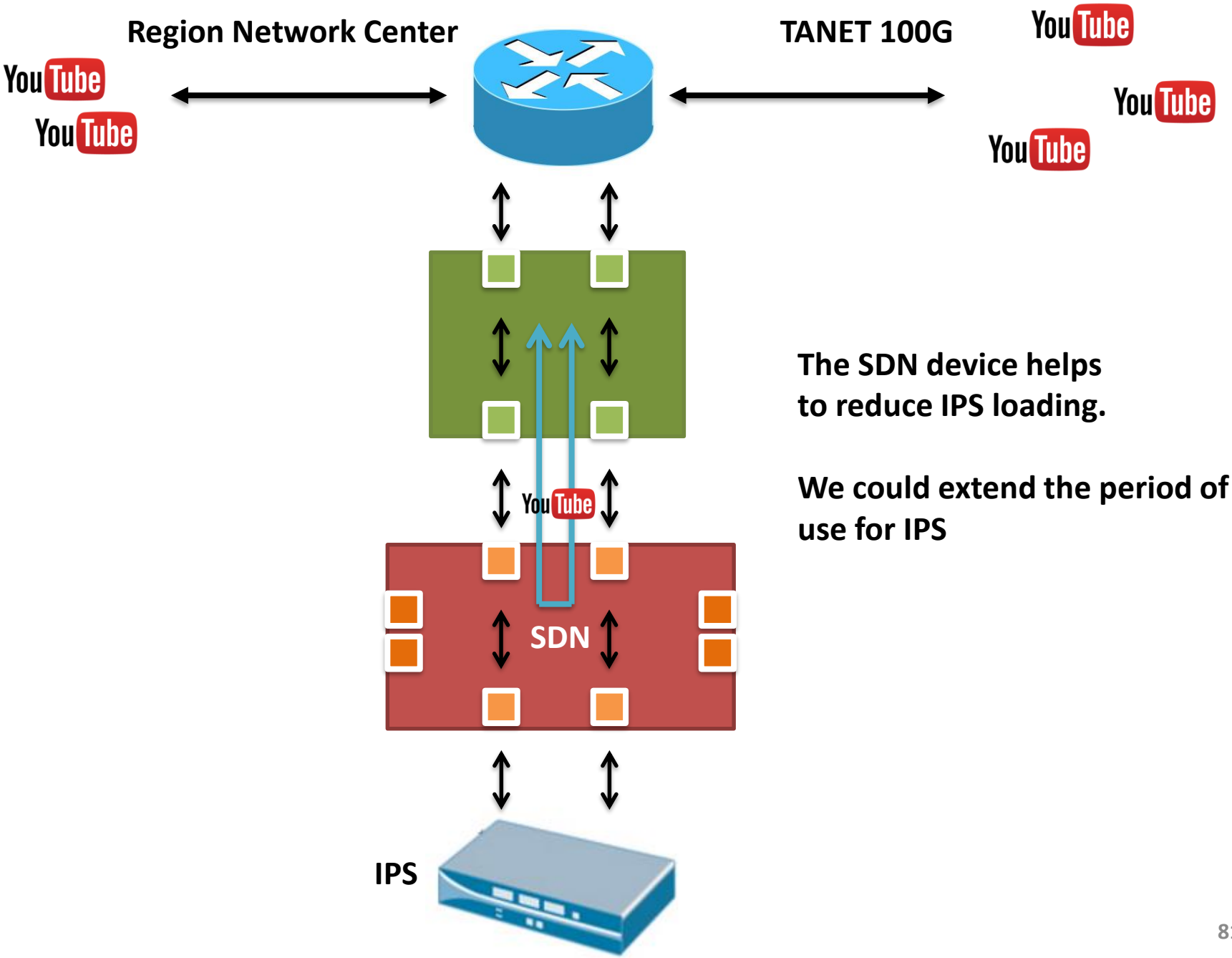


When IPS can not sustain for the network throughputs….

However, let's consider 1080P/4K YouTube video streaming:

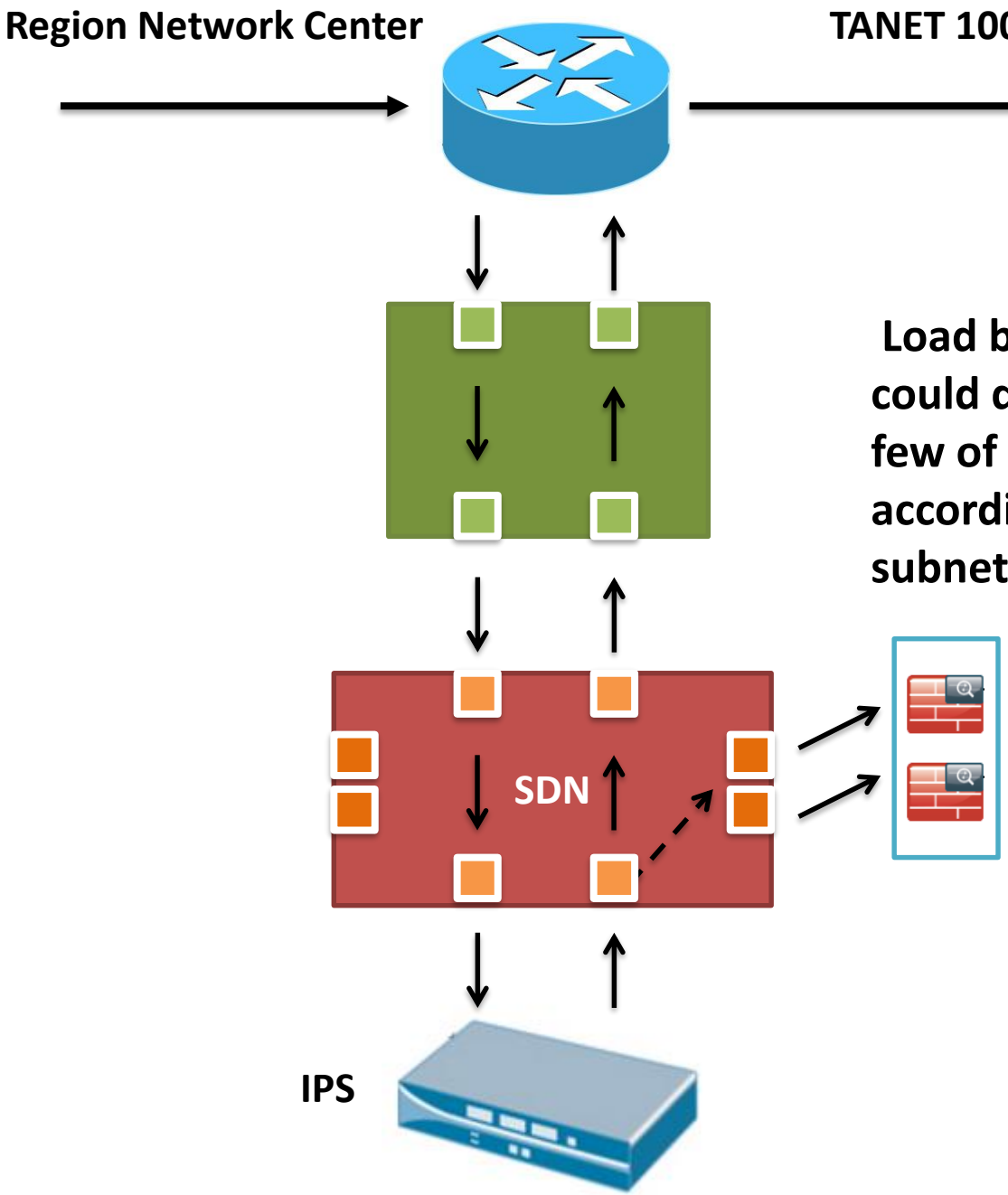
- High bandwidth
- Low risk

[Service Bypass]
The SDN device directs YouTube packets not to pass through IPS/IDS…but loop back directly

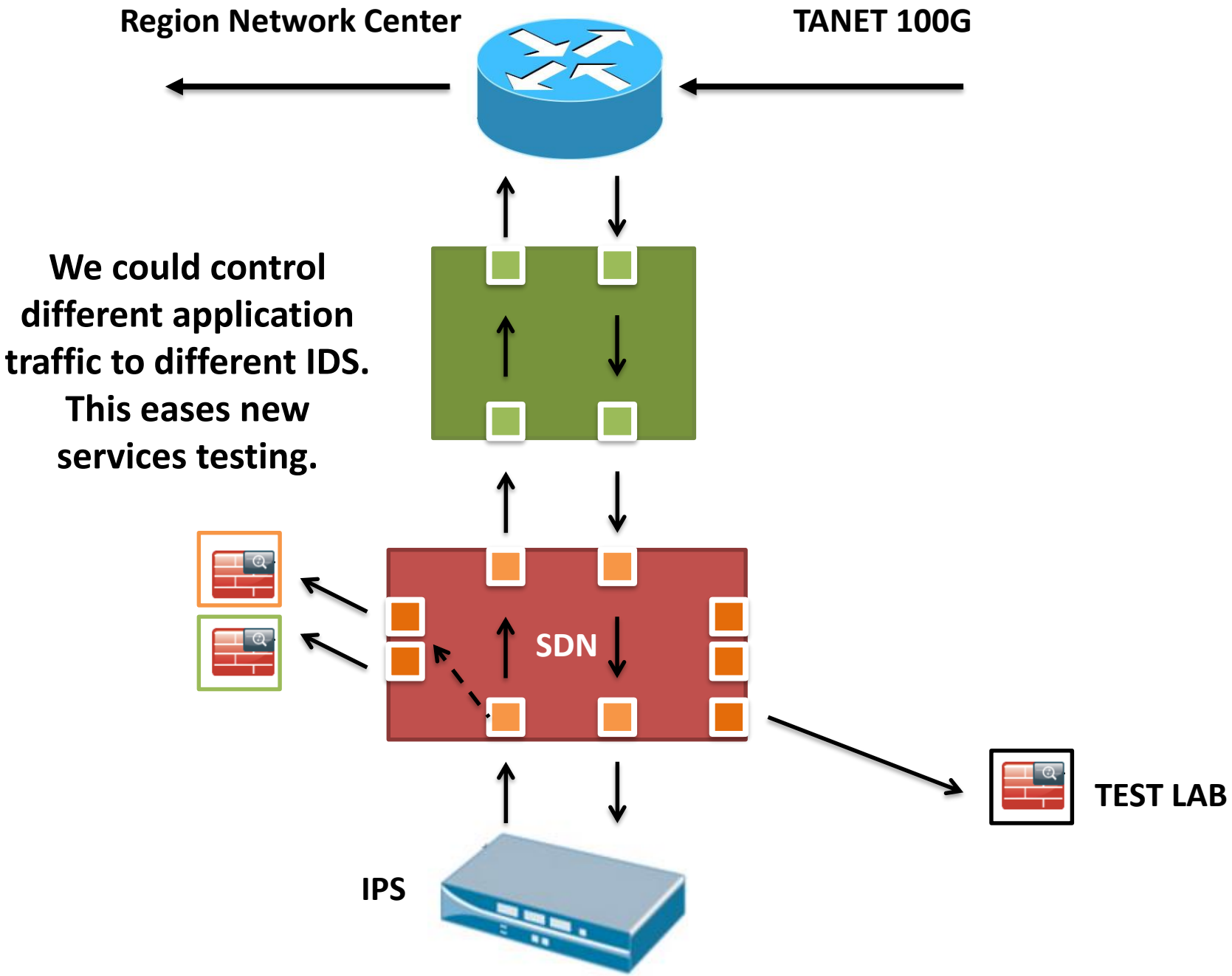


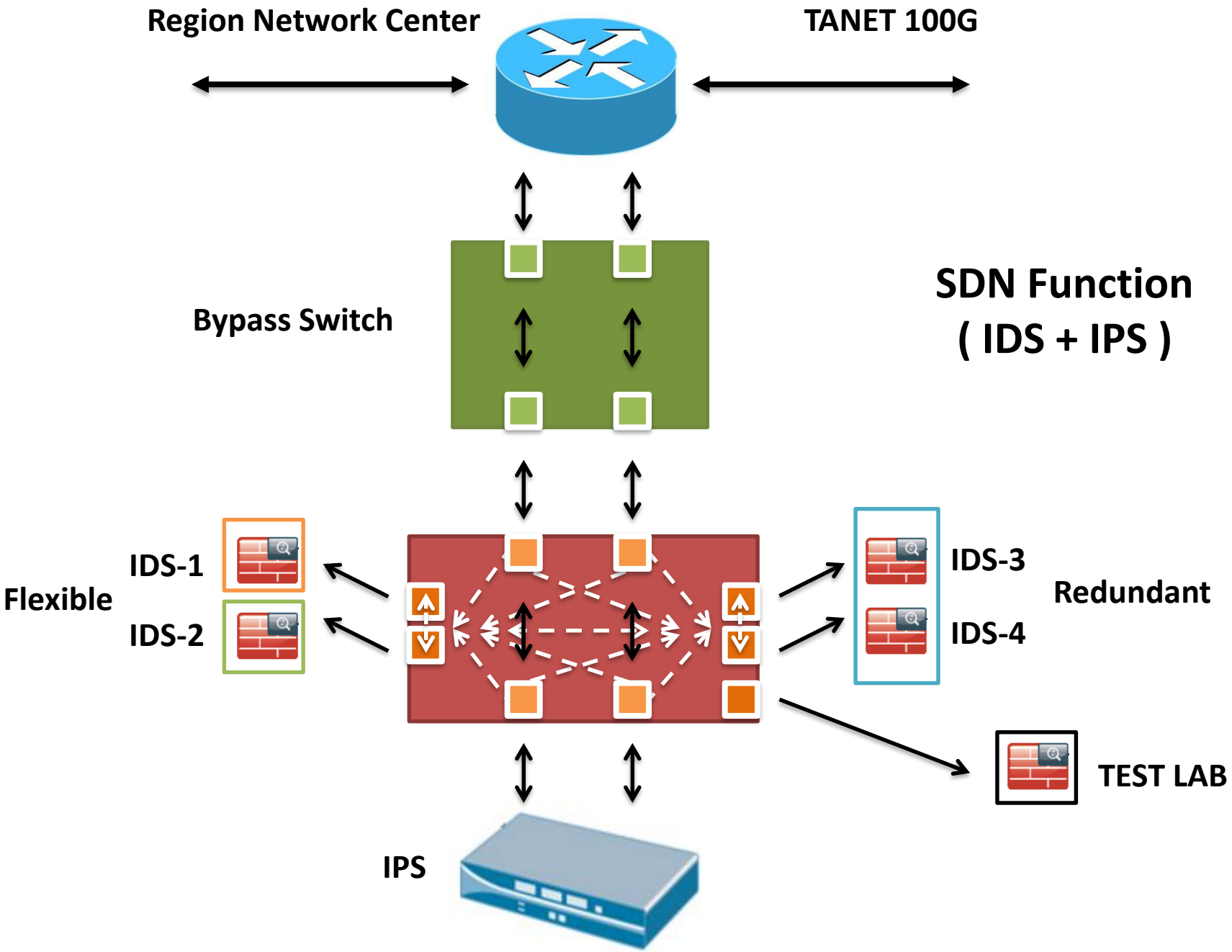
The SDN device helps to reduce IPS loading.

We could extend the period of use for IPS



Load balance function could direct traffic to a few of IDS simultaneously according to IP address / subnet/5-tuple hash

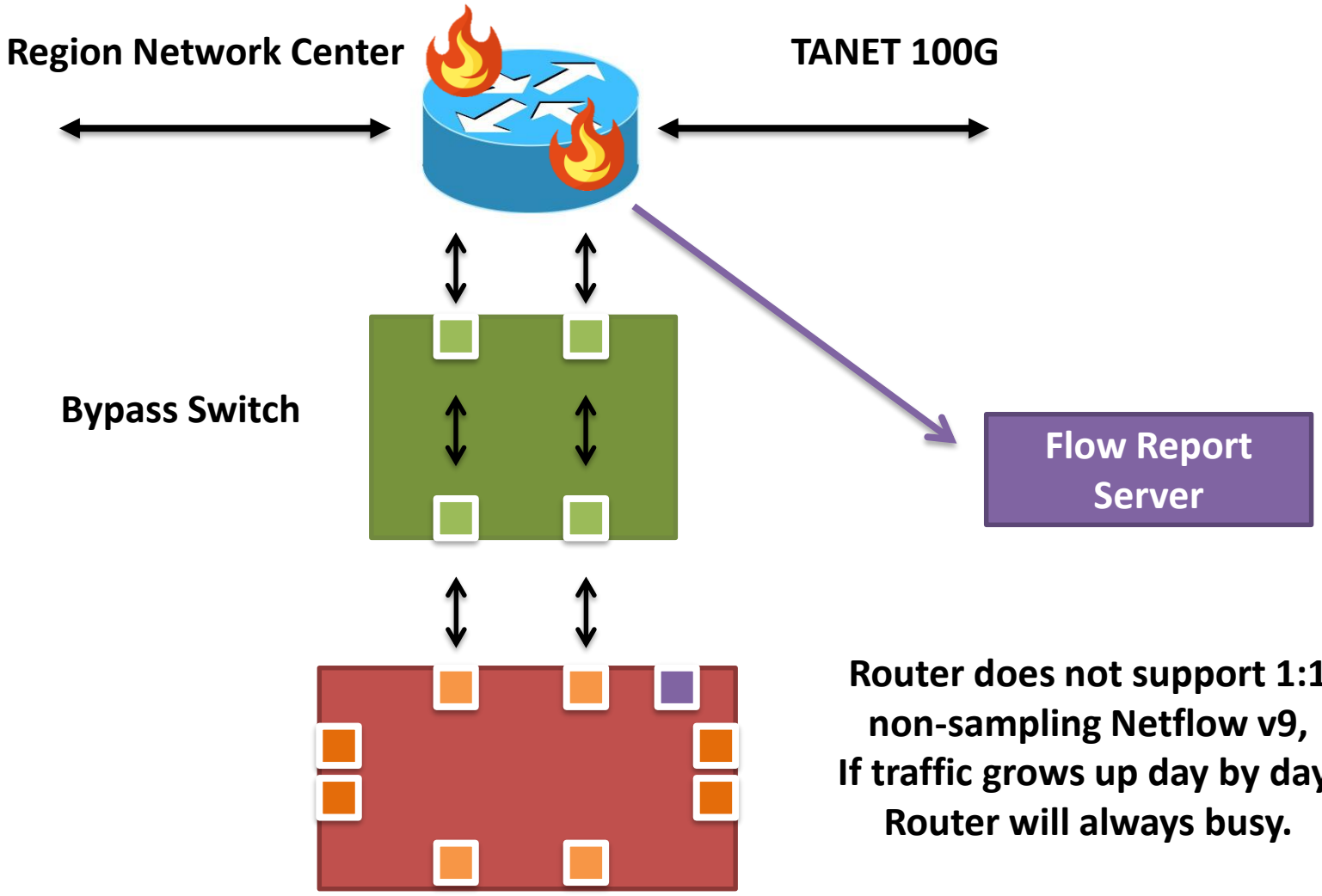

Region Network Center
TANET 100G
We could control different application traffic to different IDS. This eases new services testing.
SDN
TEST LAB
IPS


Region Network Center
TANET 100G
Bypass Switch
SDN Function
(IDS + IPS)
IDS-1
IDS-2
Flexible
IDS-3
IDS-4
Redundant
TEST LAB
IPS

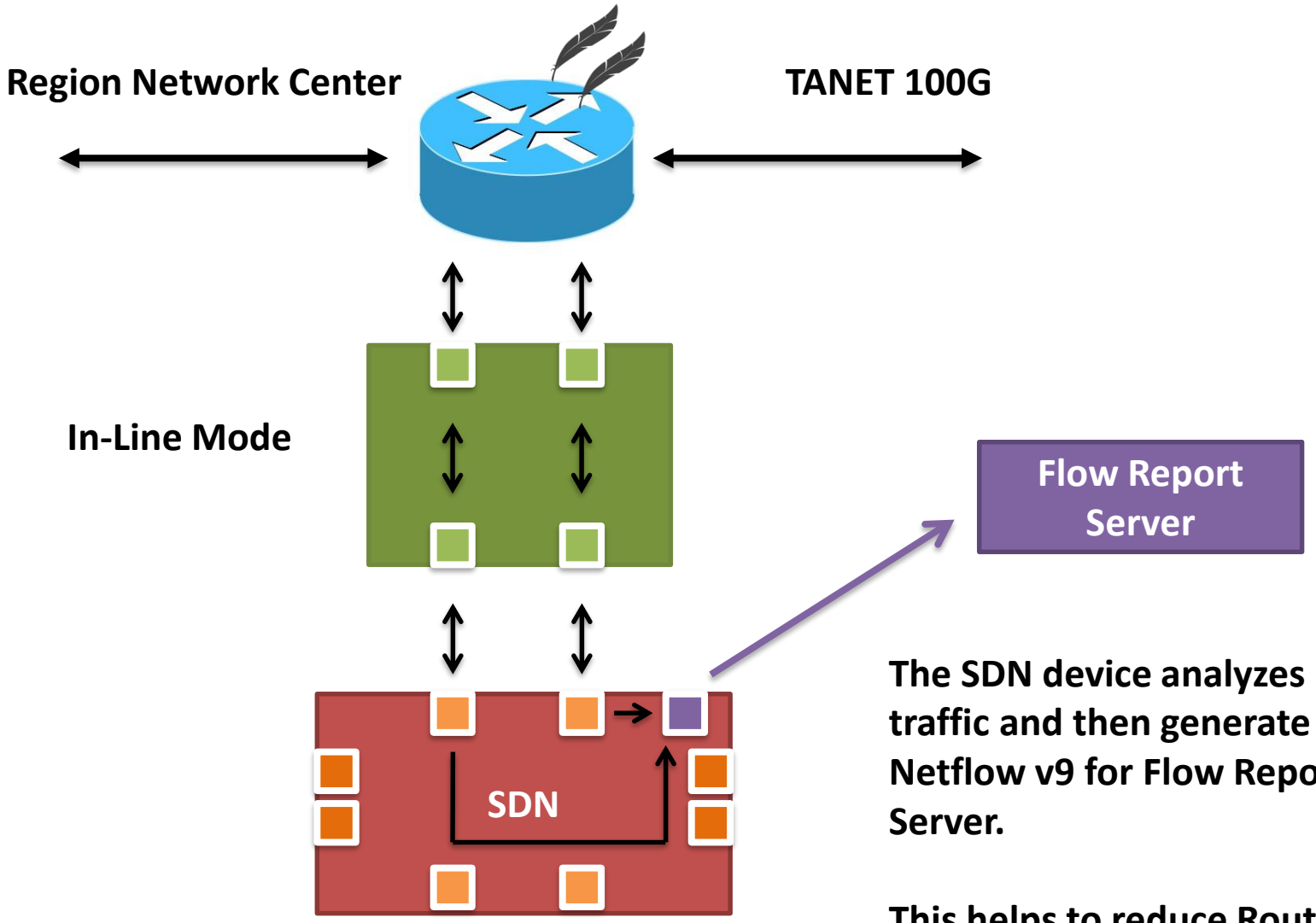
討論項目

1. SDN-based security supporting infrastructure(I)
   Network and Service bypass

2. SDN-based security supporting infrastructure(2)
   Netflow generation



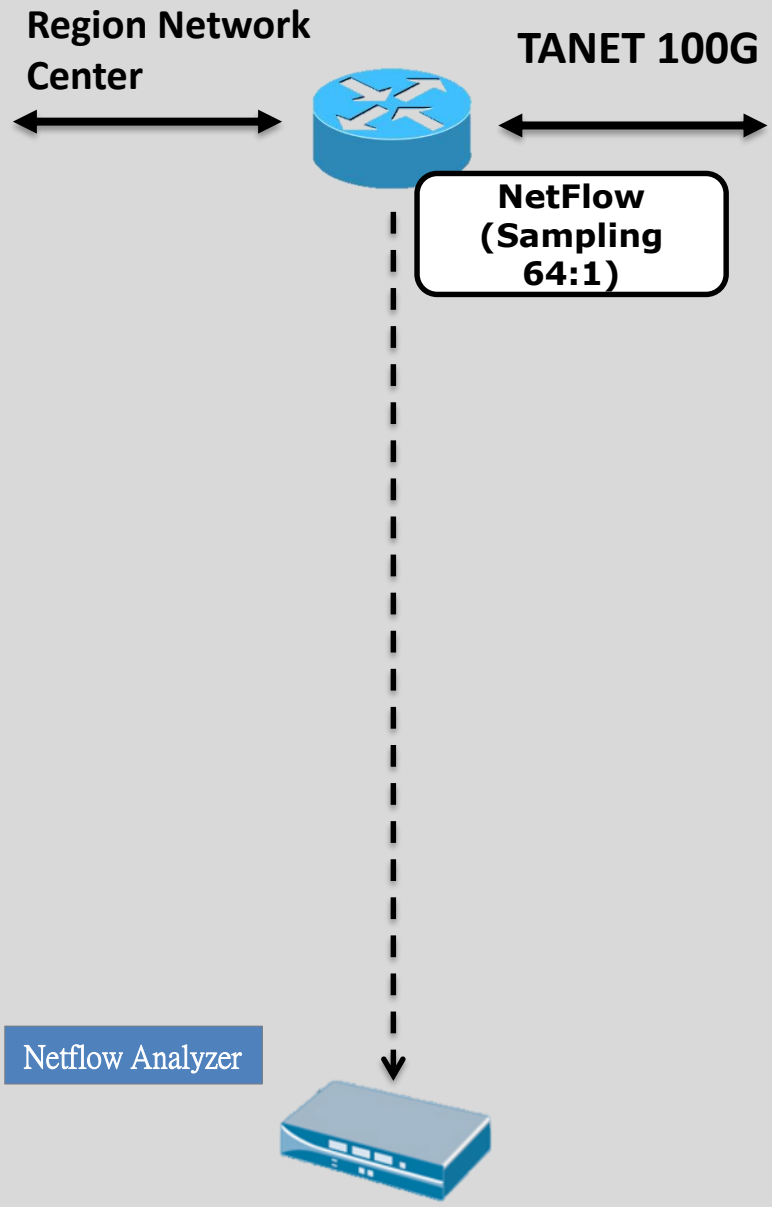
Router does not support 1:1 non-sampling Netflow v9, If traffic grows up day by day, Router will always busy.



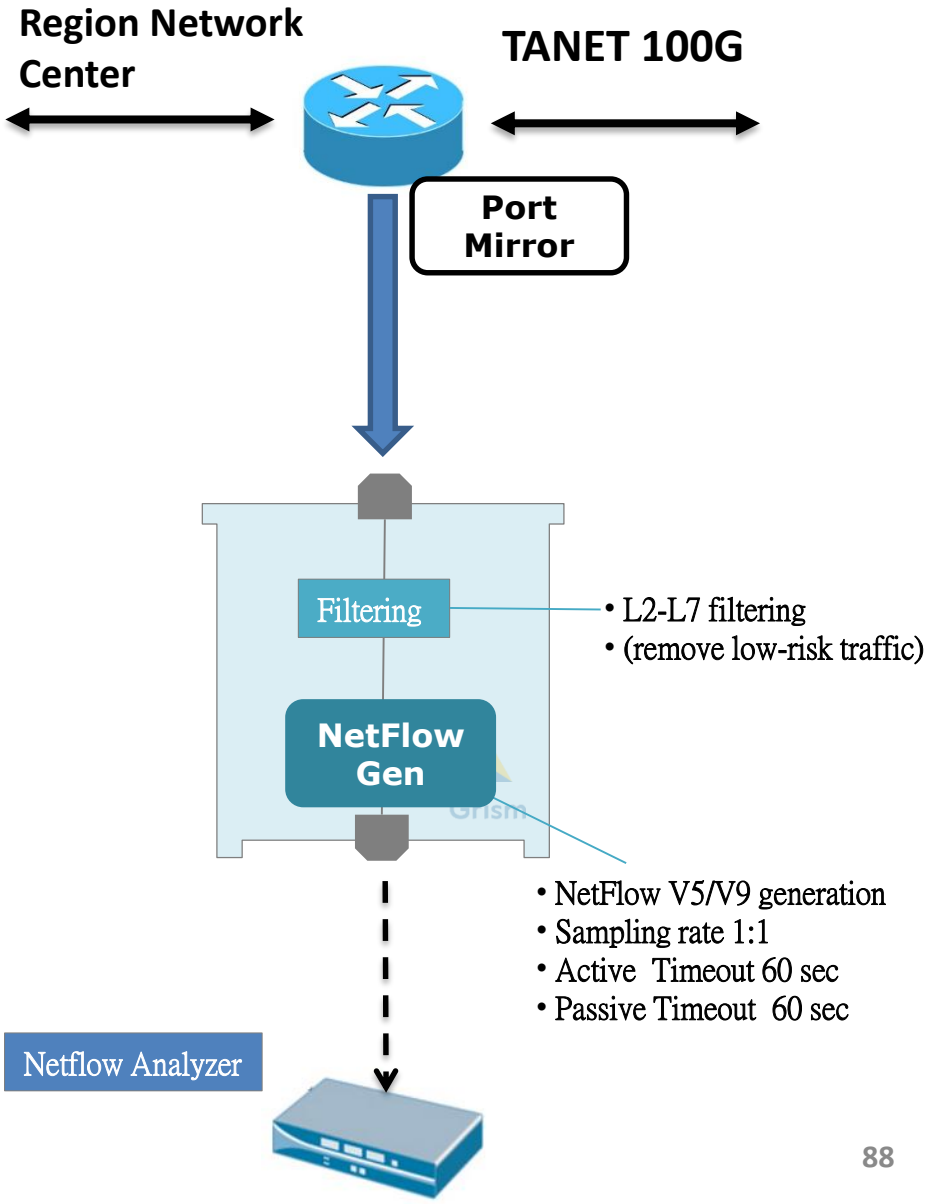
The SDN device analyzes traffic and then generate 1:1 Netflow v9 for Flow Report Server.

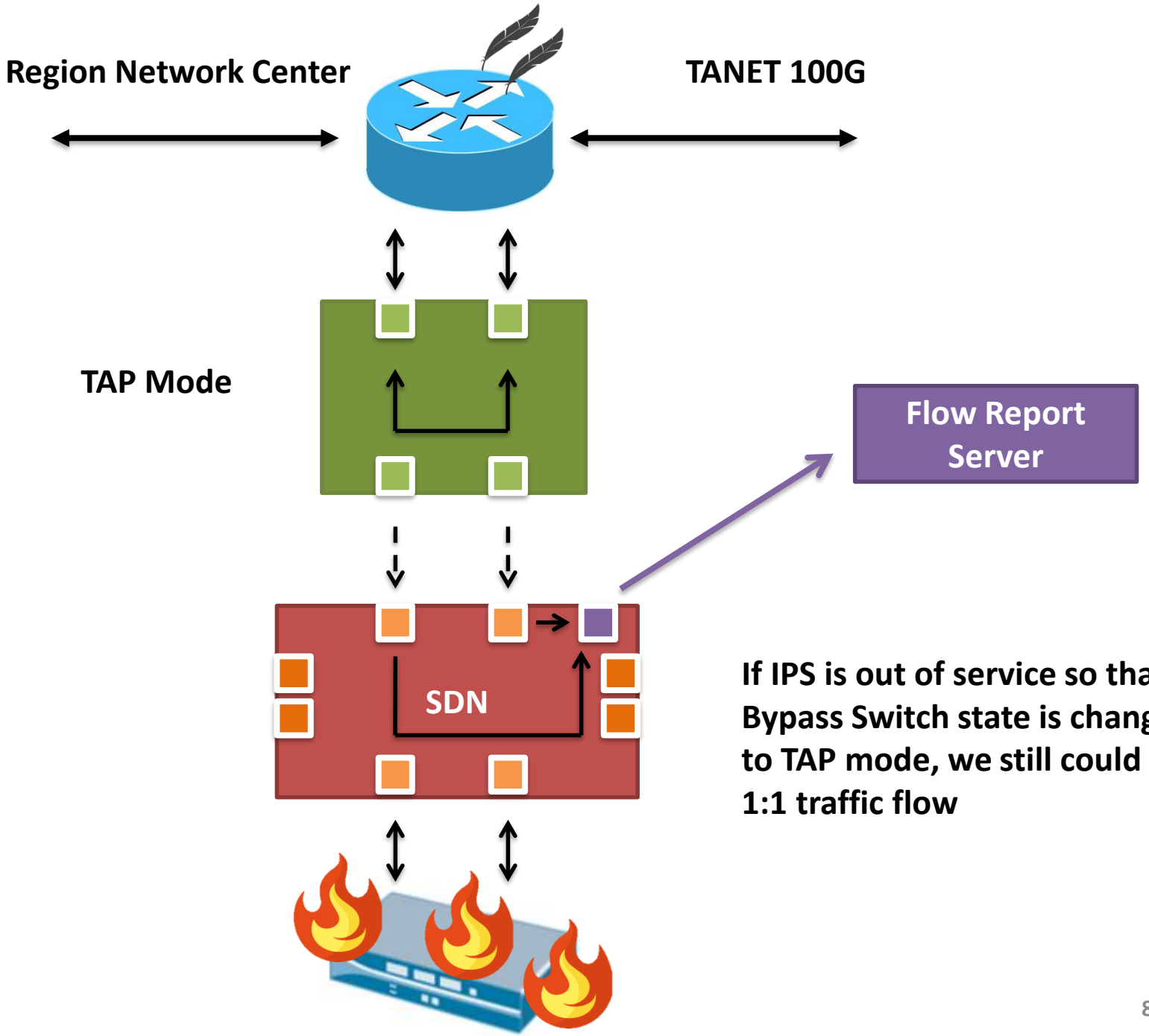
This helps to reduce Router CPU usage.

Traditional NetFlow generation architecture



New NetFlow generation architecture





If IPS is out of service so that Bypass Switch state is changed to TAP mode, we still could log 1:1 traffic flow

比較之下的優點

SDN-based Security Supporting Mechanisms

- 可用性
- 負載平衡
- 降低成本
- 彈性增加

TANET 的 Last Mile

國中小 是 TANet 數量最多的連線單位

臺灣學術網路(TANet)為了落實網路安全管理

在網路骨幹建構完整偵測與通報機制

Last Mile 的問題

各校在資安管理的自主規劃

大多是將IPS或IDS建置在校園出口

這和 TANet 資訊安全架構 有重疊之處

校園內網

資安設備大部分建置於 核心層 或 收納層

內網大量傳輸很容易造成單一節點問題

資安設備建置成本隨著使用頻寬的提升

變成一個難以解決的問題

分享運用SDN提出新的管理架構

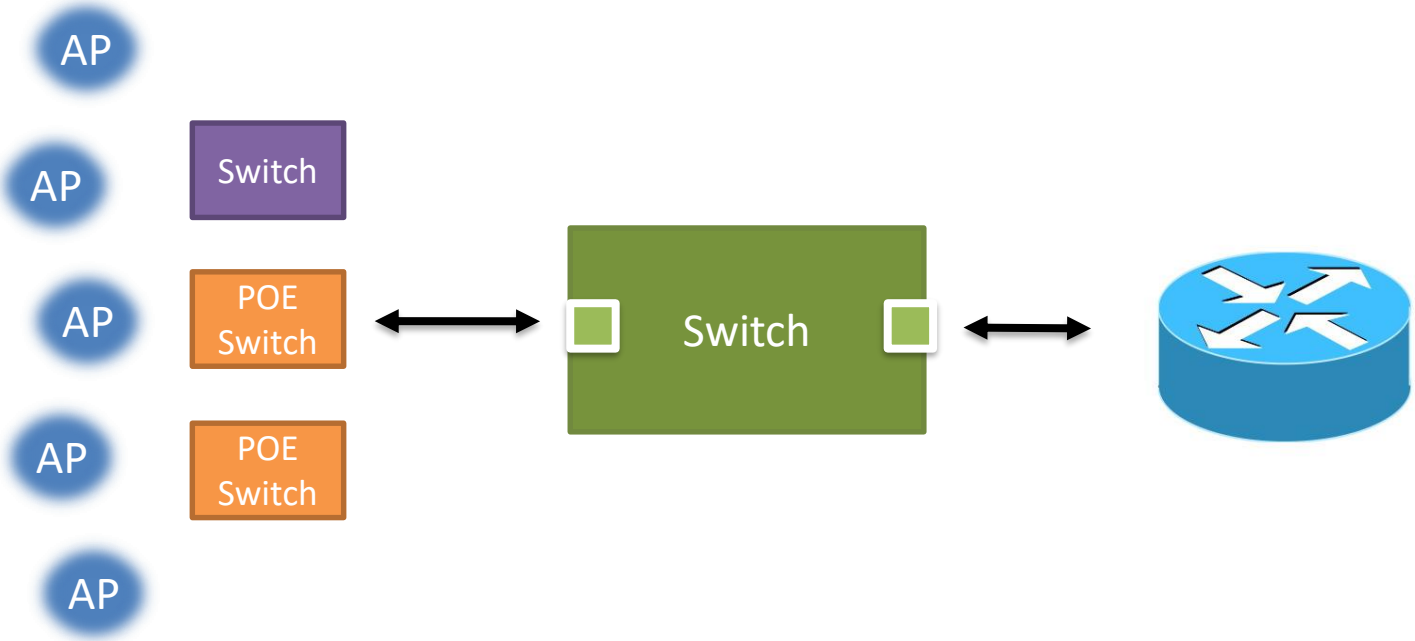
面對頻寬持續增加

資安挑戰

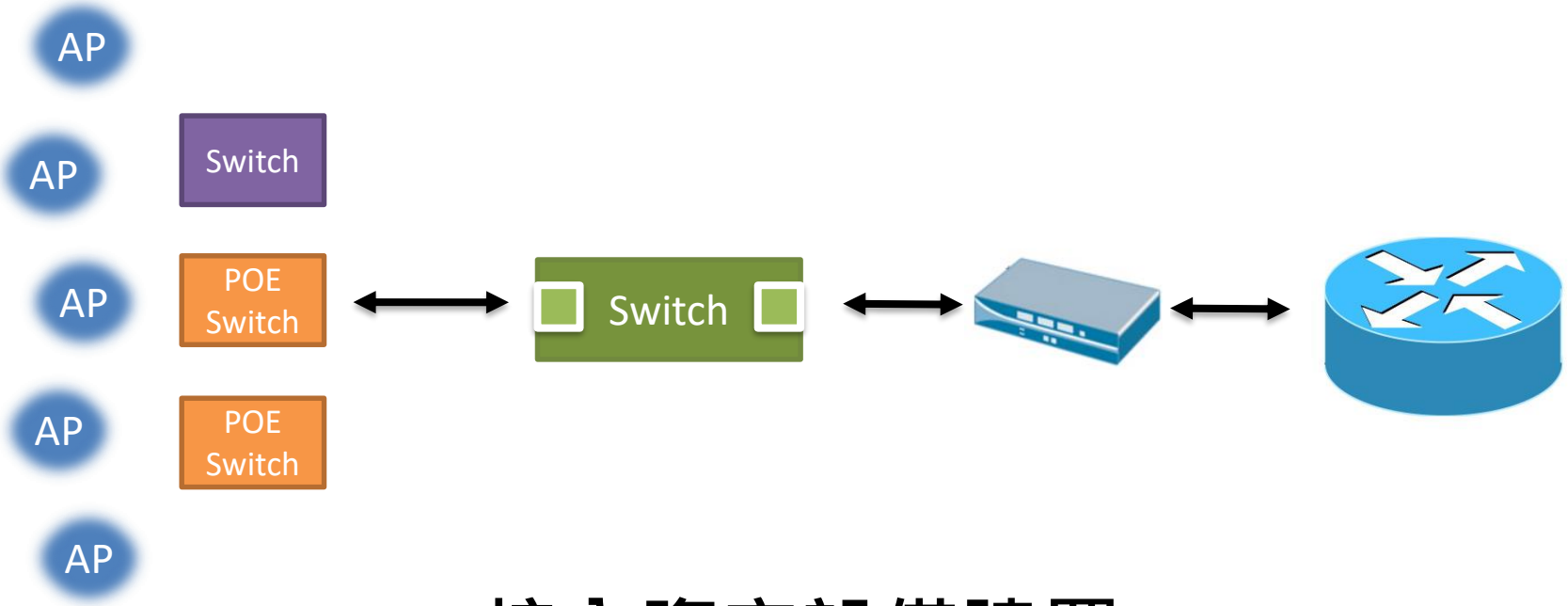
校內實測紀錄

- 地點
  - 國立暨南國際大學 管理學院
  - 無線網路使用環境
- 拓樸
  - 將 SDN Device 夾在 存取層
- 過濾內容
  - Facebook
  - Youtube

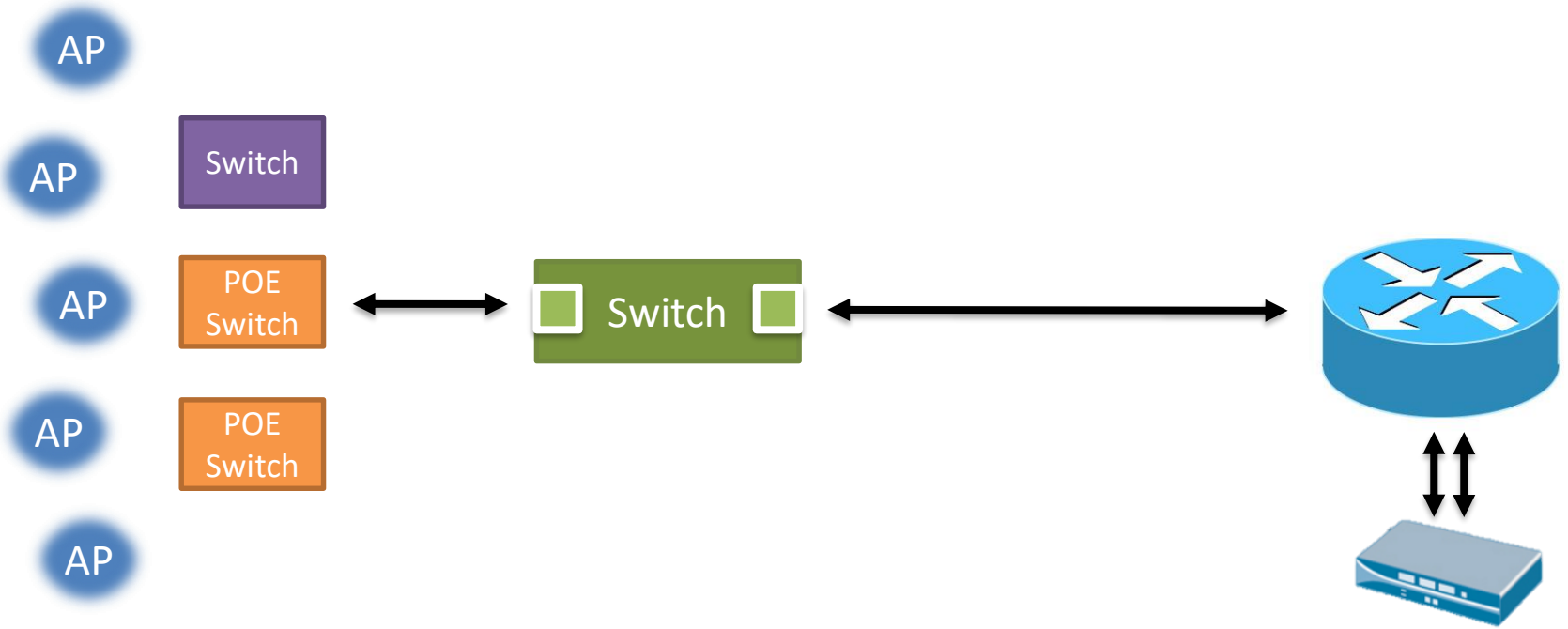
建議不同拓樸模式



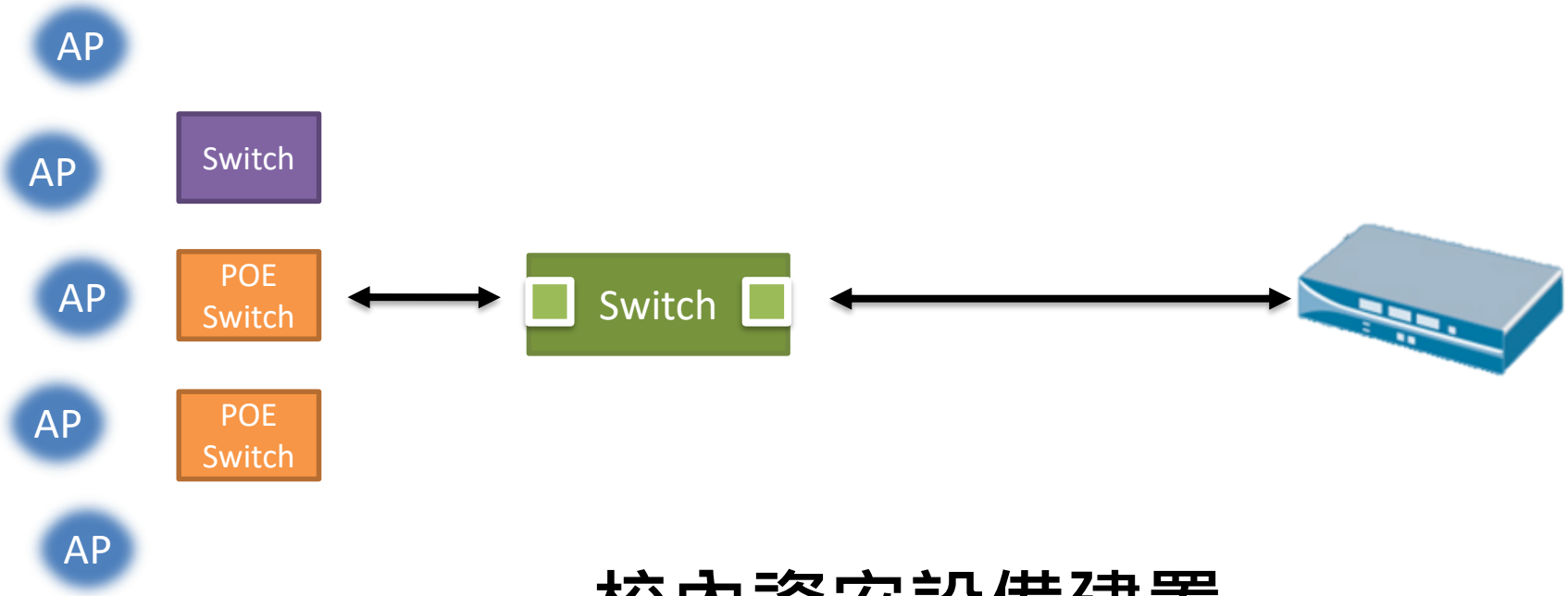
國中小 高中職常見網路拓樸



校內資安設備建置範例一

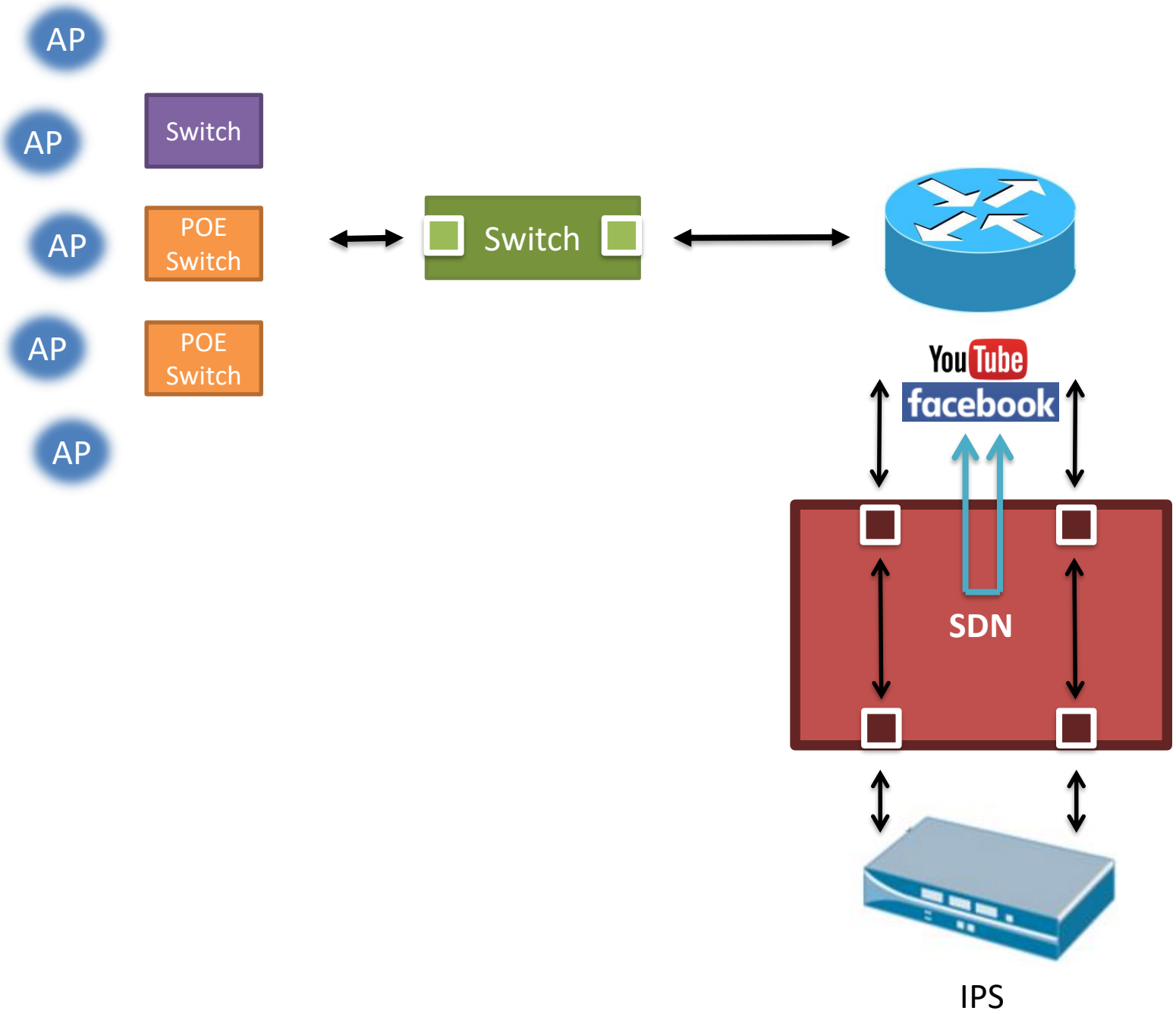


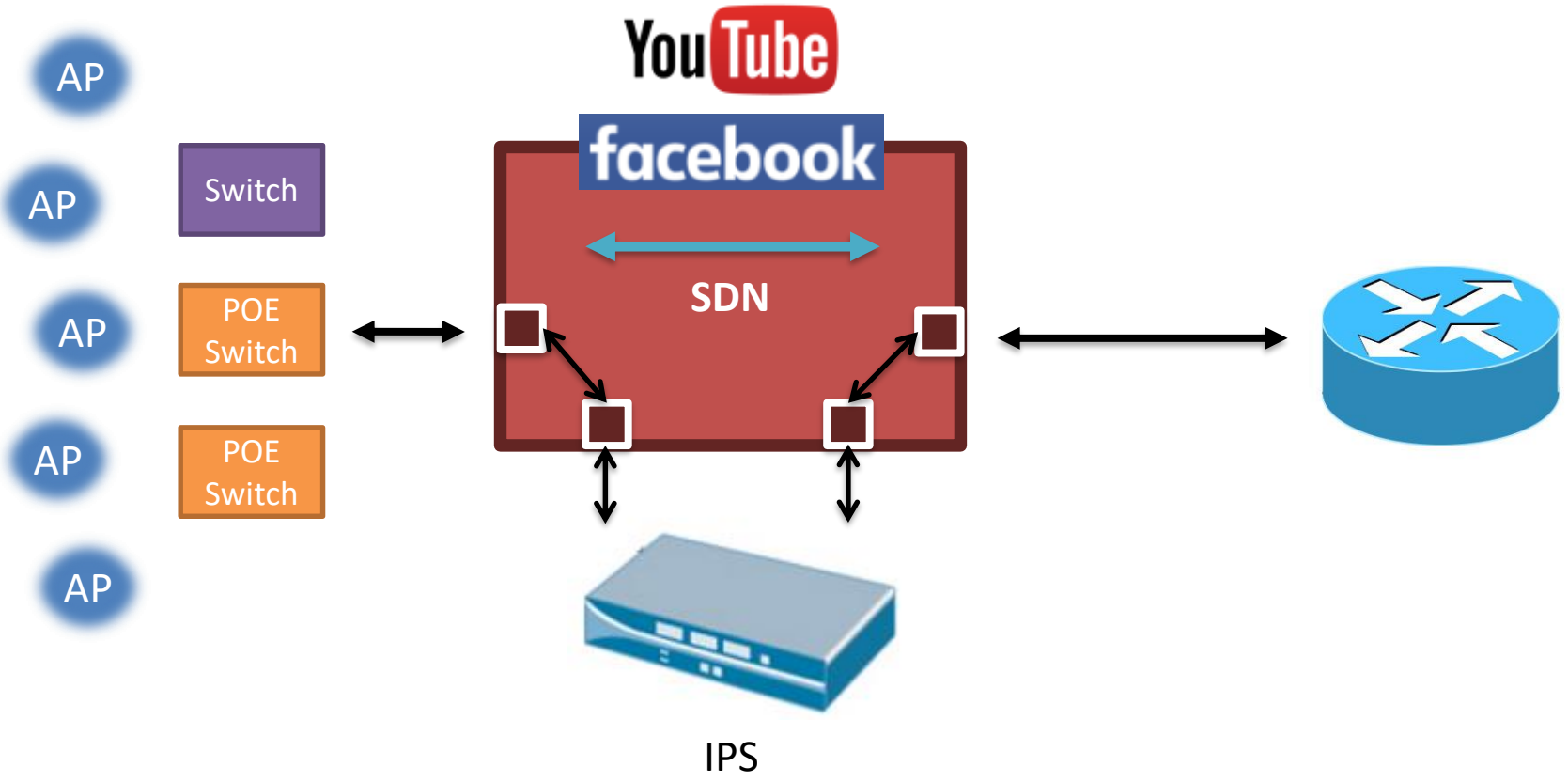
校內資安設備建置
範例二



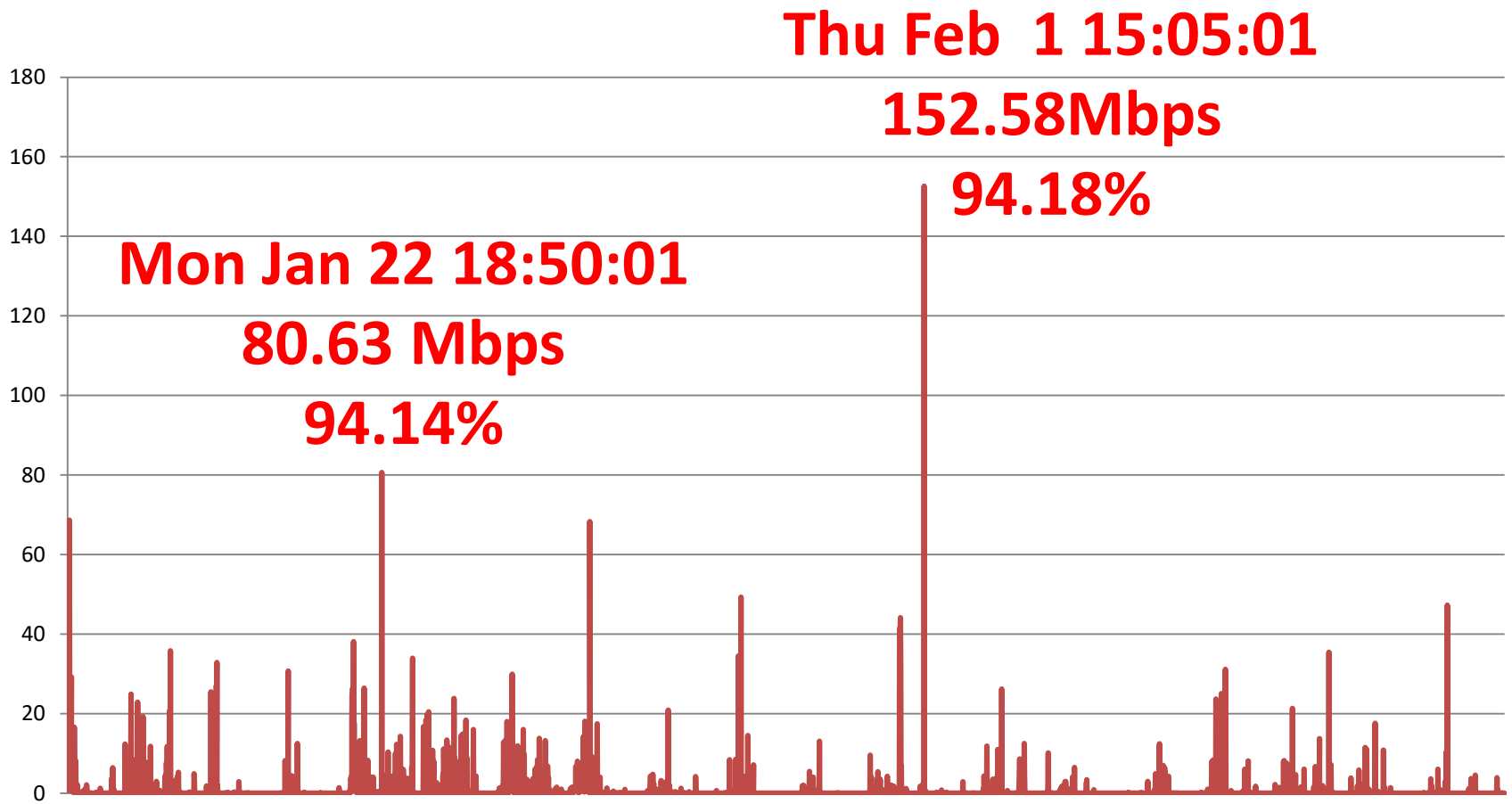
校內資安設備建置
範例三

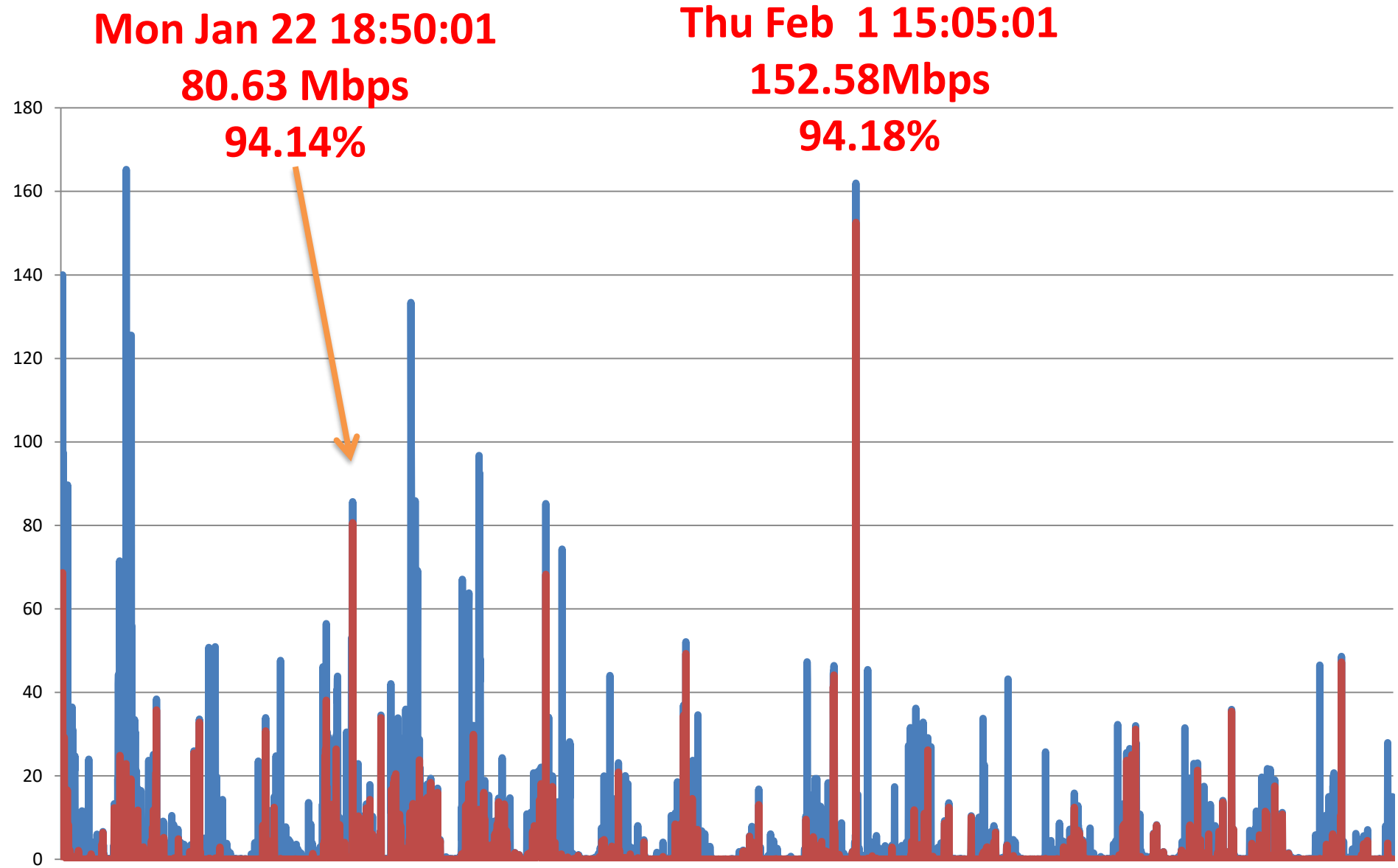
對於國中小、高中職的建議方案


AP
AP
AP
AP
AP
Switch
POE Switch
POE Switch
Switch
YouTube
facebook
SDN
IPS


AP
AP
AP
AP
AP
Switch
POE Switch
POE Switch
YouTube
facebook
SDN
IPS

FaceBook 和 Youtube 送進去 IPS 的量
01/22 18:50 濾掉 80.63 Mbps，約總流量的 94.14%
02/01 15:05 濾掉 152.58 Mbps ，約總流量的 94.18%




Mon Jan 22 18:50:01
80.63 Mbps
94.14%
Thu Feb 1 15:05:01
152.58Mbps
94.18%
180
160
140
120
100
80
60
40
20
0

IP address黑名單

- IP address 黑名單是普遍的作法
  - Gateway
  - IPS
- 透過 SDN Device 過濾異常黑名單
  - 降低 Router 和 IPS 的 Loading
  - 增加設定筆數

Domain name 過濾

- 過去
  - 透過 IP address 黑名單降低 資安風險
- 現在
  - 駭客使用 Domain name 可以不斷變更IP address

在 SDN Device 上設定阻擋已知異常 Domain name 可有效抑制 更換 IP address 的攻擊行為

Netflow 1:1紀錄

透過 Free Netflow Analyzer 收集資料

完成 1: 1 netflow 轉換

詳細記錄資訊

南投區網中心建置

Silicom Bypass Switch

PacketX 分流器

N-Cloud Flow Report

校園測試型號


PacketX
PWR
HDD
SYS
USB
BYPASS
CONSOLE
USB
RESET
P0
P1
P2
P3
P4
P5
P6
P7
MGMT

繼續不斷嘗試不同做法

Syslog-ng 架設輔助式管理

SYSLOG-NG Server 安裝流程

A. **Install EPEL Repositories:**

01. Login to your server as root (or su root)
02. Type: cd /root
03. Type (Current link as of this post):

```
wget http://dl.fedoraproject.org/pub/epel/6Server/i386/epel-relea
```

wget http://dl.fedoraproject.org/pub/epel/6Server/i386/epel-release-6-8.noarch.rpm

04. Type: rpm -Uvh /root/epel-release-6-8.noarch.rpm

05. To verify the software repository was installed type: yum repolist

You should see something like:

```
[root@myserver ~]# yum repolist
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.cisp.com
 * epel: mirror.metrocast.net
 * extras: mirror.symnds.com
 * updates: mirrors.easynews.com
repo id                         repo name
base                            CentOS-6 - Base
epel                            Extra Packages for Enterprise Linux 6
extras                          CentOS-6 - Extras
updates                         CentOS-6 - Updates
repolist: 13,225
```

B. **Install Syslog-NG:**

01. Run an update check: yum check-update

    To see if this will impact any other software on your system.

02. Check the availability of Syslog-NG by typing: yum list *syslog-ng*

```
[root@myserver ~]# yum list *syslog-ng*
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.cisp.com
 * epel: fedora.westmancom.com
 * extras: mirror.symnds.com
 * updates: mirrors.easynews.com
Available Packages
syslog-ng.i686                                  3.2.5-3.el6
syslog-ng-devel.i686                            3.2.5-3.el6
syslog-ng-libdbi.i686                           3.2.5-3.el6
```

03. Install both ***syslog-ng and syslog-ng-libdbi*** (to avoid an error message) by typing: yum install syslog-ng syslog-ng-libdbi
(Of course, you could install everything... if you want to...)

```
[root@myserver ~]# yum install syslog-ng syslog-ng-libdbi
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.cisp.com
 * epel: archive.linux.duke.edu
 * extras: mirror.symnds.com
 * updates: mirrors.easynews.com
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package syslog-ng.i686 0:3.2.5-3.el6 will be installed
--> Processing Dependency: libnet.so.1 for package: syslog-ng-3.2
--> Processing Dependency: libevtlog.so.0 for package: syslog-ng-
---> Package syslog-ng-libdbi.i686 0:3.2.5-3.el6 will be installe
--> Processing Dependency: libdbi.so.0 for package: syslog-ng-lib
--> Running transaction check
---> Package eventlog.i686 0:0.2.12-1.el6 will be installed
---> Package libdbi.i686 0:0.8.3-4.el6 will be installed
---> Package libnet.i686 0:1.1.5-1.el6 will be installed
--> Finished Dependency Resolution
```

```
Dependencies Resolved

================================================================================
 Package                        Arch              Version
================================================================================
Installing:
 syslog-ng                      i686              3.2.5-3.el6
 syslog-ng-libdbi               i686              3.2.5-3.el6
Installing for dependencies:
 eventlog                       i686              0.2.12-1.el6
 libdbi                         i686              0.8.3-4.el6
 libnet                         i686              1.1.5-1.el6

Transaction Summary
================================================================================
Install       5 Package(s)

Total download size: 583 k
Installed size: 1.7 M
Is this ok [y/N]: y
```

If prompted to to import a GPG key... type: y

```
warning: rpmts_HdrFromFdno: Header V3 RSA/SHA256 Signature, key I
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
Importing GPG key 0x0608B895:
 Userid : EPEL (6)
 Package: epel-release-6-8.noarch (installed)
 From   : /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
Is this ok [y/N]: y
```

C. **Configure CentOS Services, Stop Rsyslog, and Start Syslog-NG:**

01. Disable **rsyslog**: chkconfig rsyslog off
02. Confirm **rsyslog** is disabled:

```
[root@myserver ~]# chkconfig --list rsyslog
rsyslog         0:off   1:off   2:off   3:off   4:off   5:off   6
```

03. Enable **syslog-ng**: chkconfig syslog-ng on
04. Confirm **syslog-ng** is enabled:

```
[root@myserver ~]# chkconfig --list syslog-ng
syslog-ng               0:off   1:off   2:on    3:on    4:on    5
```

05. Stop Rsyslog:

```
[root@myserver ~]# service rsyslog stop
Shutting down system logger:                               [  OK
```

06. Start Syslog-NG:

```
[root@myserver ~]# service syslog-ng start
Starting syslog-ng:                                        [  OK
```

D. **Example Configuration for Syslog-NG:**

01. Add the following to the END of **/etc/syslog-ng/syslog-ng.conf**:

```
# My Switches
source s_cisco {
        udp(ip(0.0.0.0) port(514));
        tcp(ip(0.0.0.0) port(514));
};

destination d_cisco {
        file(
                "/var/log/cisco/$HOST-$YEAR$MONTH$DAY.log"
                perm(644)
                create_dirs(yes)
        );
};

log { source(s_cisco); destination(d_cisco); };
```

編輯 IPv4 防火牆

vi /etc/sysconfig/iptables

加入以下兩行
-A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

重啟服務
/etc/init.d/iptables restart

```
[root@ip212 home]# /etc/init.d/iptables restart
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
```

編輯 IPv6 防火牆

vi /etc/sysconfig/ip6tables

加入以下兩行
-A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p ipv6-icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 546 -d fe80::/64 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp6-adm-prohibited
-A FORWARD -j REJECT --reject-with icmp6-adm-prohibited
COMMIT
```

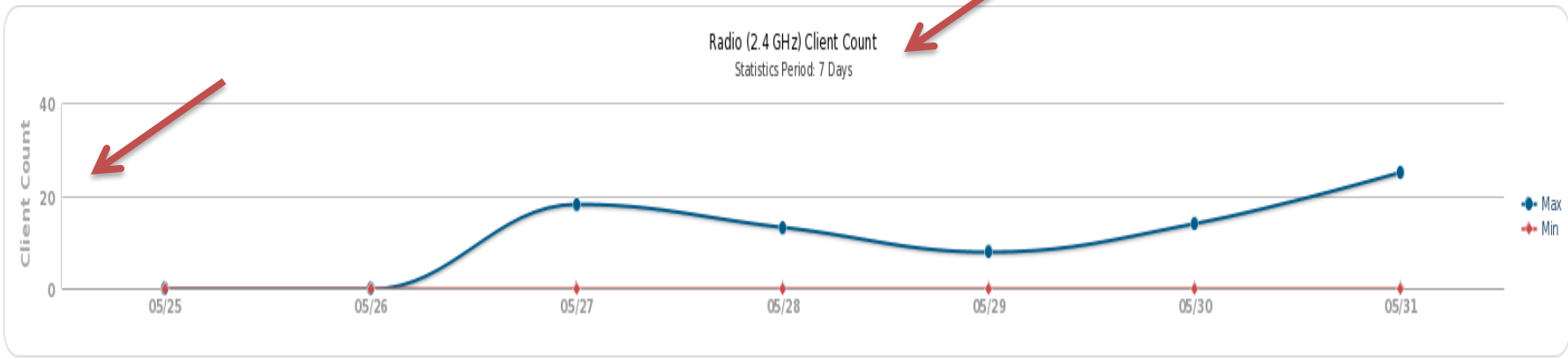
重啟服務
/etc/init.d/ip6tables restart

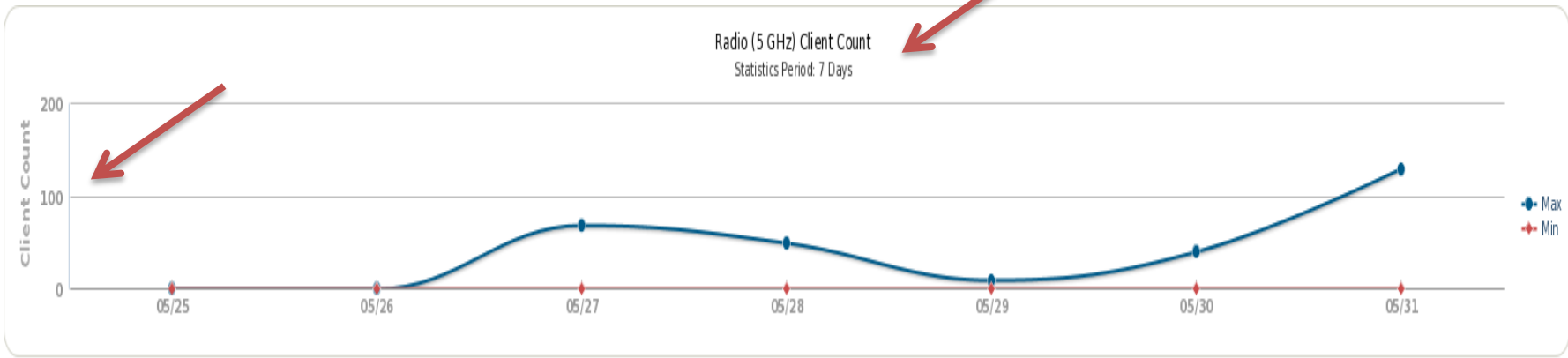
```
[root@ip212 home]# /etc/init.d/ip6tables restart
ip6tables: Setting chains to policy ACCEPT: filter          [  OK  ]
ip6tables: Flushing firewall rules:                         [  OK  ]
ip6tables: Unloading modules:                               [  OK  ]
ip6tables: Applying firewall rules:                         [  OK  ]
```

國立暨南國際大學
National Chi Nan University

校園無線網路
發展與建置規劃分享

今年六月份紀錄


Radio (2.4 GHz) Client Count
Statistics Period: 7 Days
Client Count
40
20
0
05/25
05/26
05/27
05/28
05/29
05/30
05/31
Max
Min


Radio (5 GHz) Client Count
Statistics Period: 7 Days
Client Count
200
100
0
05/25
05/26
05/27
05/28
05/29
05/30
05/31
Max
Min

Wi-Fi Alliance

在 2018 年 10 月
正式宣布新的命名規範

802.11n	→	Wi-Fi 4
802.11ac	→	Wi-Fi 5
802.11ax	→	Wi-Fi 6

Generation of network connection	Sample user interface visual
Wi-Fi 6	
Wi-Fi 5	
Wi-Fi 4	

過去的標準

802.11

802.11b

802.11g/a

不再給予新的名稱

~~Wi-Fi 1 / 2 / 3~~

通訊協定標準	簡稱	2.4GHz	5GHz	6GHz	最高傳輸速度
802.11		●			2Mbit/s
802.11b		●			11Mbit/s
802.11g/a		● (g)	● (a)		54Mbit/s
802.11n	Wi-Fi 4	●	●		72Mbit/s (20 MHz) 150Mbit/s (40 MHz)
802.11ac	Wi-Fi 5	●	●		
802.11ax	Wi-Fi 6	●	●	●	

2.4GHz 和 5GHz 有何差異?

資料來源：科技新報

無線電波 每秒流向改變次數

Hz　在 1 秒以下流向改變次數

G　為 1,000 的 3 次方

2.4GHz / 5GHz　→　2400000000 / 5000000000

部分頻段無須額外特許證照或費用給三個類別使用

工業（Industrial）

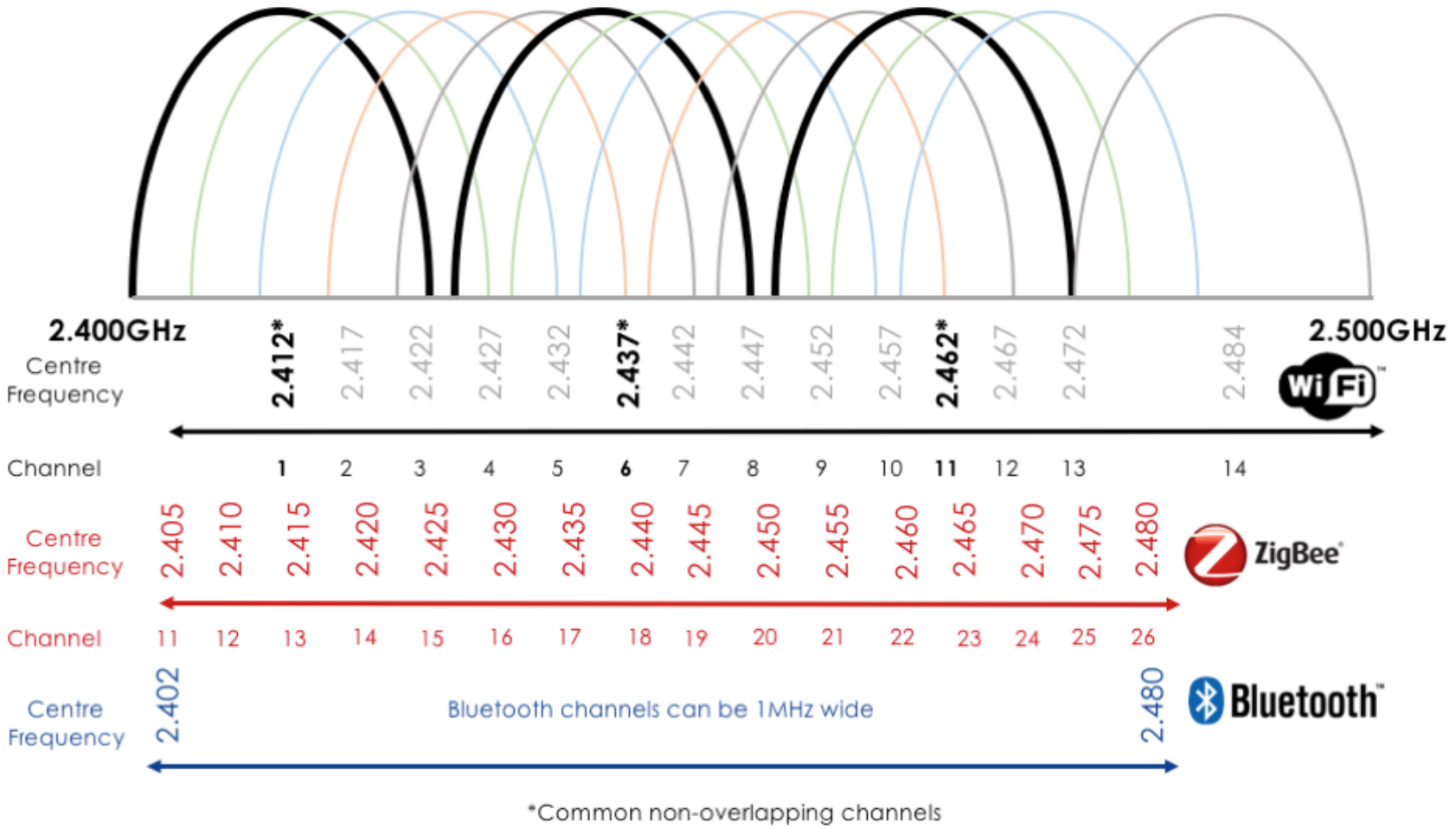
科學（Scientific）

醫學（Medical）

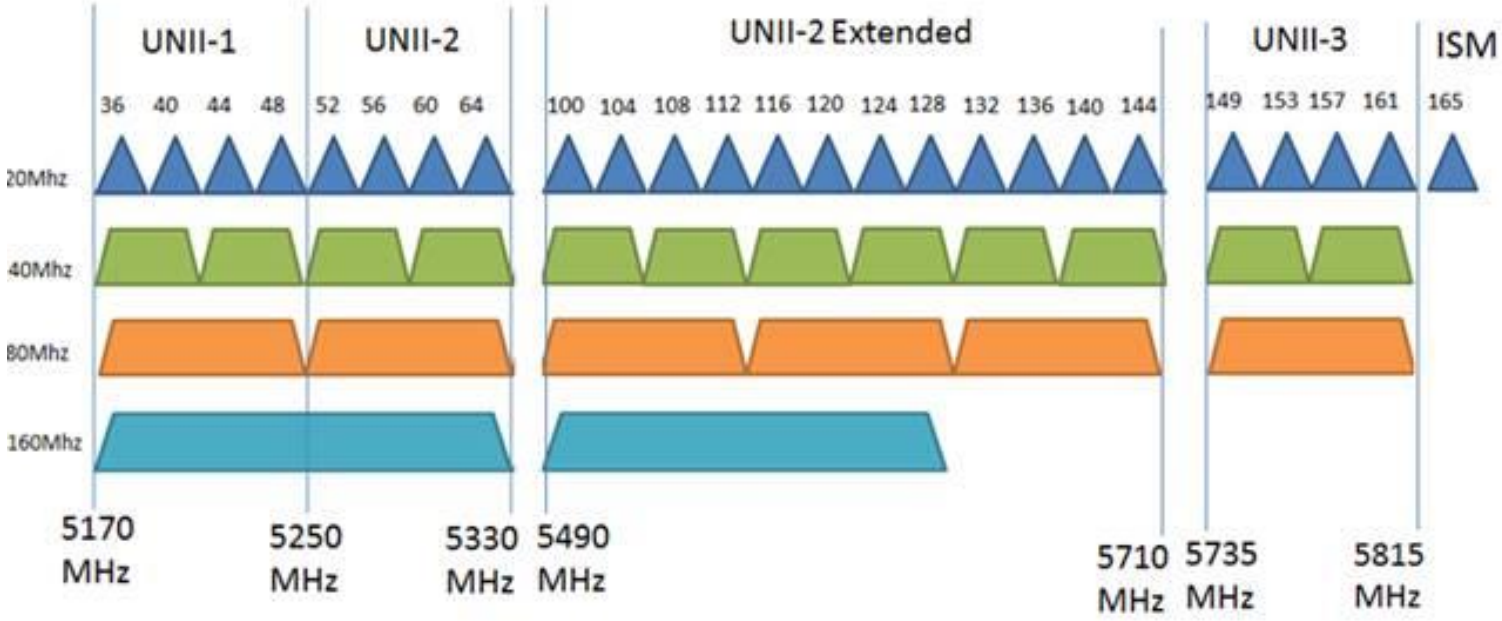
2.4GHz / 5GHz 傳輸距離　→　1.0 倍 / 0.5 倍

仍受到空間影響

2.4 GHz 的問題


2.400GHz
Centre Frequency
2.412*
2.417
2.422
2.427
2.432
2.437*
2.442
2.447
2.452
2.457
2.462*
2.467
2.472
2.484
2.500GHz
Wi Fi
Channel
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Centre Frequency
2.405 2.410 2.415 2.420 2.425 2.430 2.435 2.440 2.445 2.450 2.455 2.460 2.465 2.470 2.475 2.480
ZigBee
Channel
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
Centre Frequency
2.402
Bluetooth channels can be 1MHz wide
2.480
Bluetooth
*Common non-overlapping channels

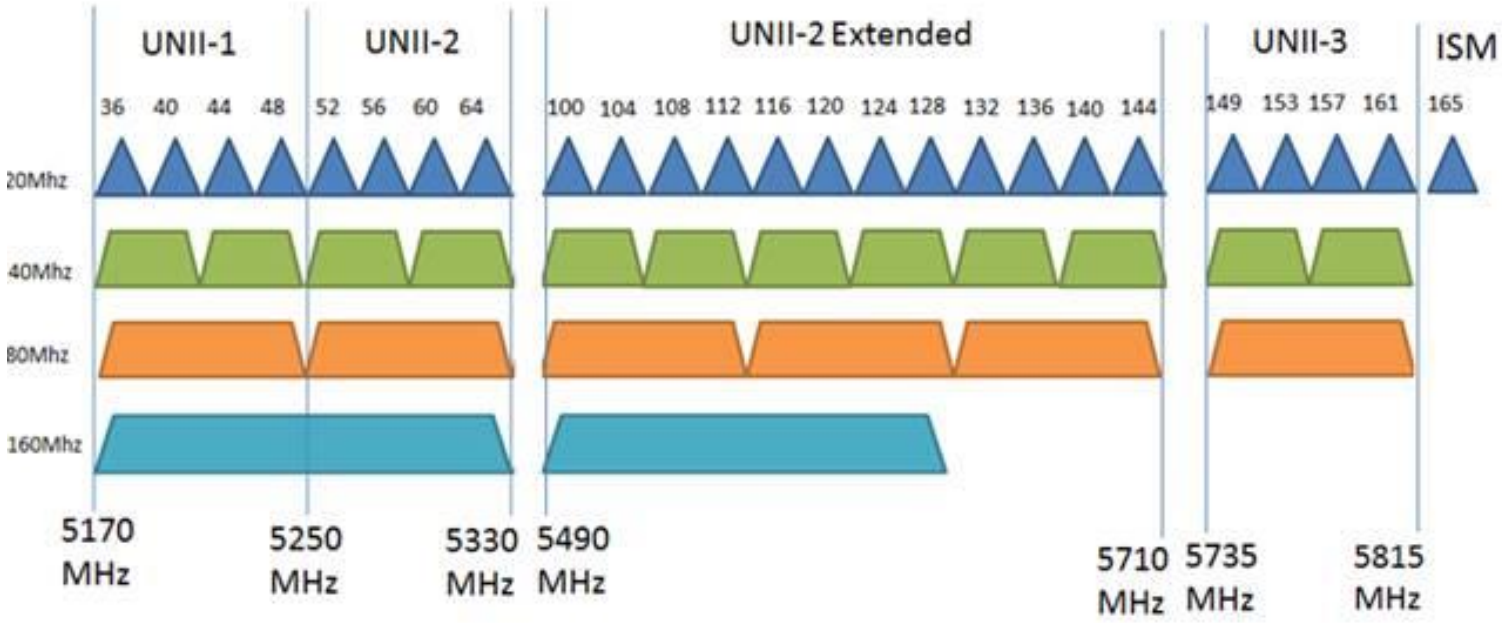
5 GHz 的問題



舊款僅少數設備支援　舊款支援

衛星訊號傳輸和機場氣象雷達

5 GHz 頻段



160MHz 160MHz 80MHz

2.4 GHz / 5GHz 整合問題

- 是否設定相同SSID
- 連線選擇上的問題
- 韌體升版可否改善
- 自動連線設定

高增益 / 主動式

高增益	主動式
被動	主動
方向性加強	電力放大訊號

魚與熊掌是否可以兼得?

MIMO

自802.11n 開始

出現一個新功能

可透過多組天線傳輸進行傳輸

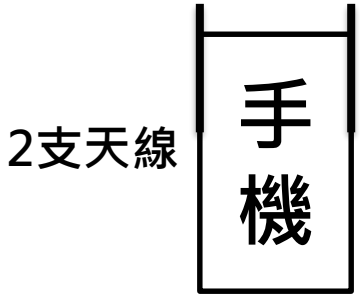
Multi-Input Multi-Output (MIMO)

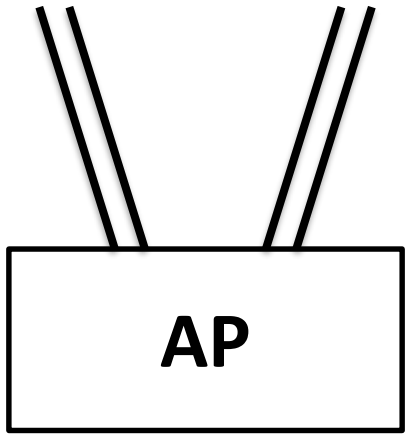
多輸入多輸出

MIMO

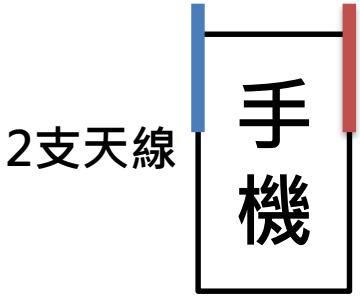
802.11n	單支天線	最高傳輸天線數量	最高傳輸速率
	150 Mbps	4	600 Mbps

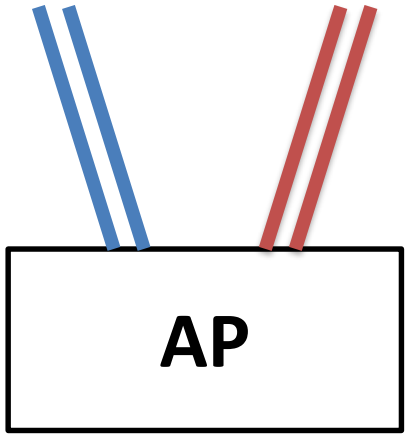
802.11ac	單支天線	最高傳輸天線數量	最高傳輸速率
	867 Mbps	8	6.934 Gbps





4支天線





2送 + 2收

加強傳輸品質或穩定訊號

	802.11ac	802.11ax
頻帶	5 GHz	2.4 GHz 與 5 GHz
通道頻寬	20 MHz、40 MHz、80 MHz、80+80 MHz 與 160 MHz	20 MHz、40 MHz、80 MHz、80+80 MHz 與 160 MHz
FFT 大小	64, 128, 256, 512	256, 512, 1024, 2048
子載波間距	312.5 kHz	78.125 kHz
OFDM 符碼持續期間	3.2 us + 0.8/0.4 us CP	12.8 us + 0.8/1.6/3.2 us CP
最高調變	256-QAM	1024-QAM
資料速率	433 Mbps (80 MHz，1 SS) 6933 Mbps (160 MHz，8 SS)	600.4 Mbps (80 MHz，1 SS) 9607.8 Mbps (160 MHz，8 SS)

Beamforming 波束成型

802.11n 開始成形，但因各家廠牌標準不一
尚未普及

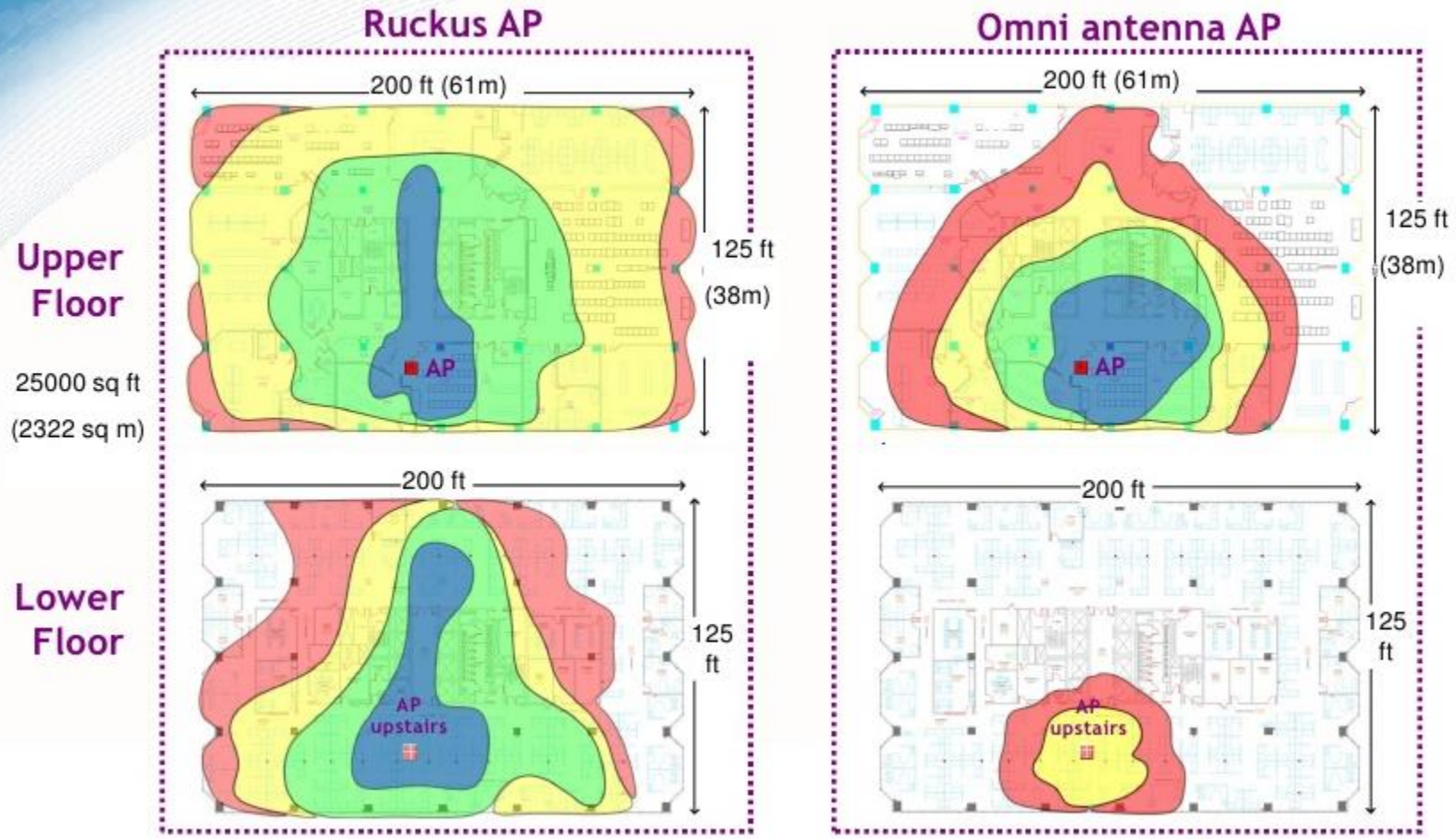
802.11ac 趨近於統一運作模式
已經普及

Beamforming 波束成型

訊號彼此之間會有干擾、抵消等現象

Beamforming 波束成型
透過計算讓訊號傳輸方式改變
提升傳輸速率、品質、距離

Performance and Coverage Advantage



Source: North-American Carrier Test Location: Commercial high rise building in Canada

802.11ax

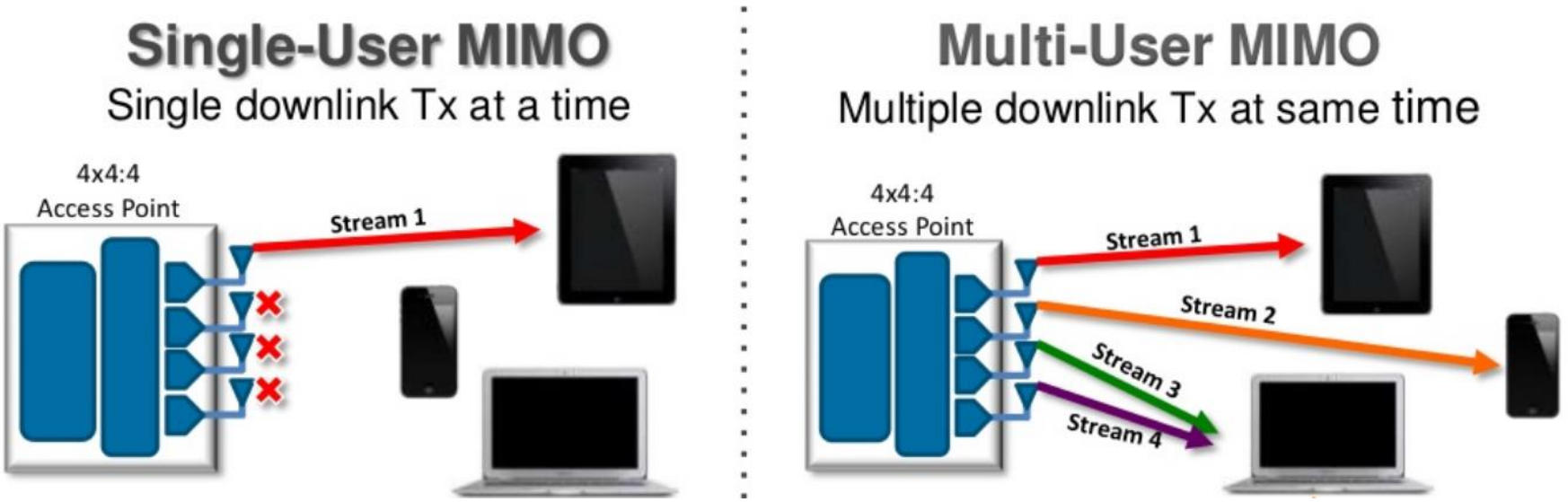
資料來源

電腦王、每日頭條、PCM

MU-MIMO

以 MIMO 和 Beamforming 為基礎
提出了 MU-MIMO (Multi-User)

Source：Ruckus



MU-MIMO的限制

	下載	上傳
802.11ac	√	
802.11ax	√	√

OFDM / OFDMA

Source：Wi-Fi Alliance

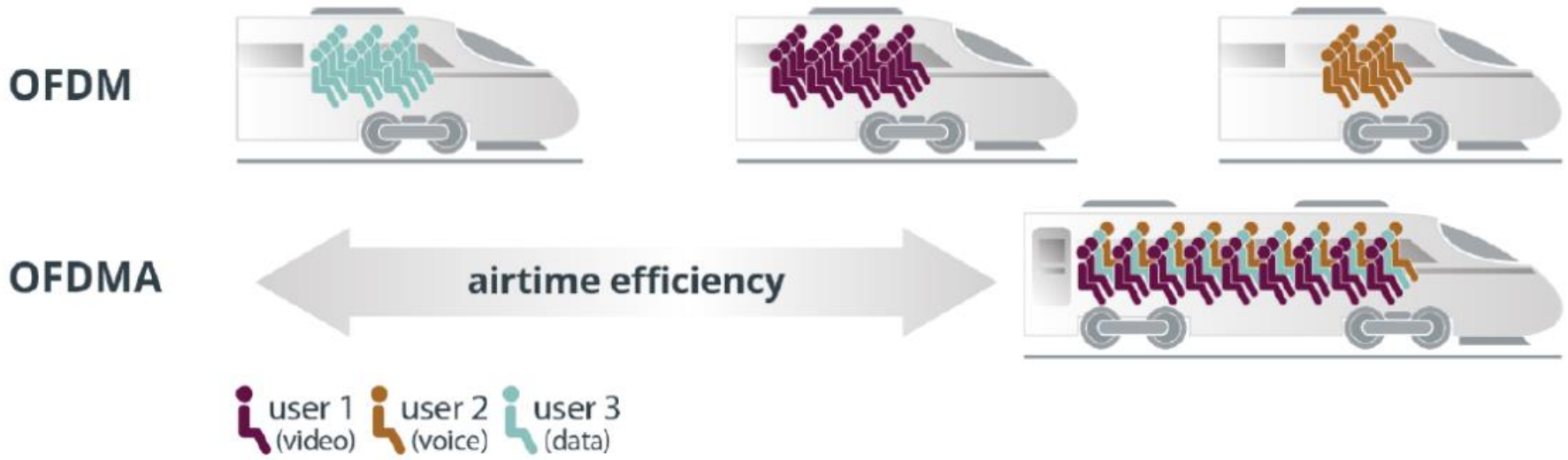


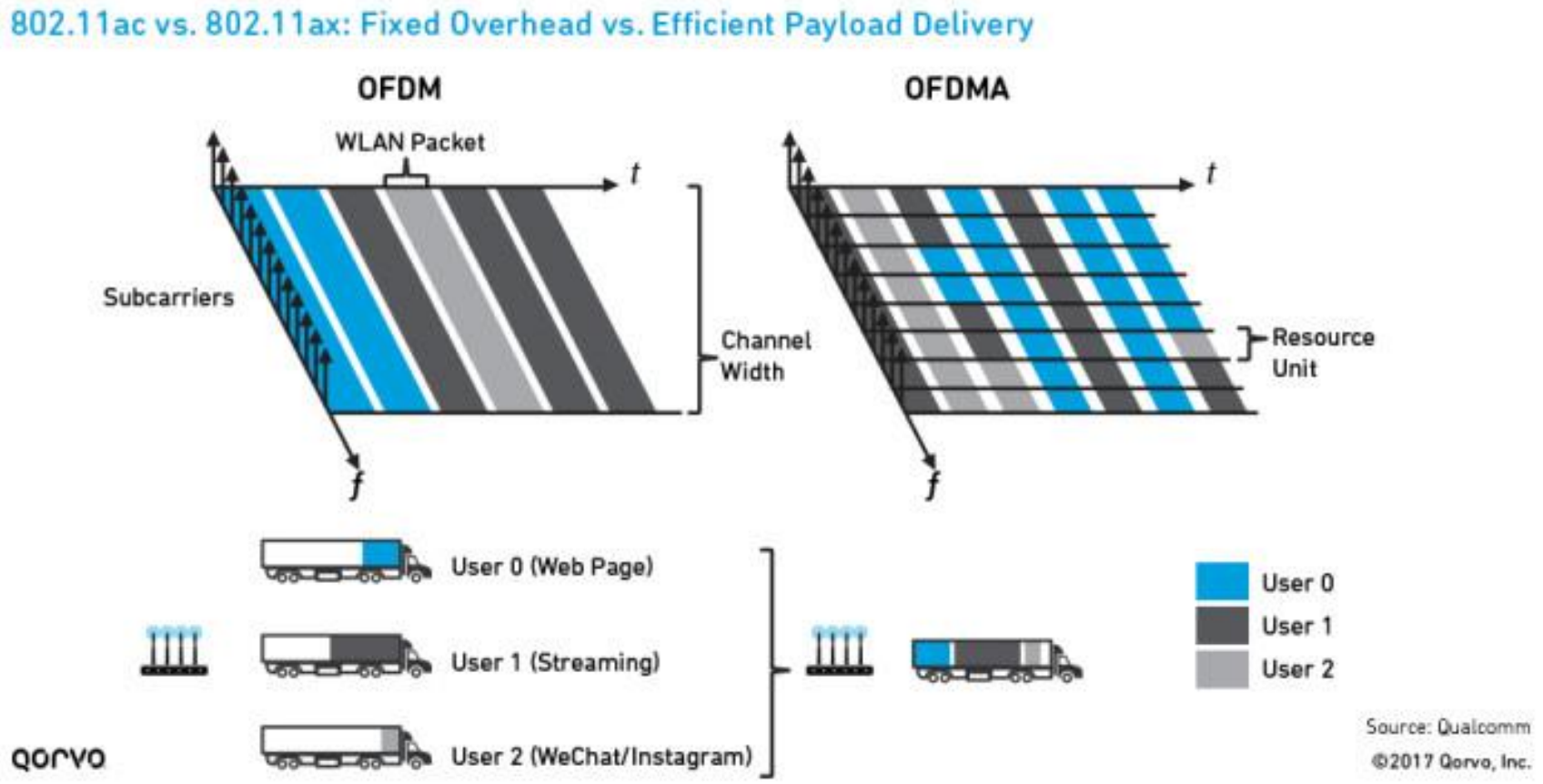
Figure 1. OFDMA in Wi-Fi 6 allows multiple users with different traffic profiles to transmit simultaneously over the same channel

OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access

OFDM / OFDMA

Source：Qorvo / Qualcomm

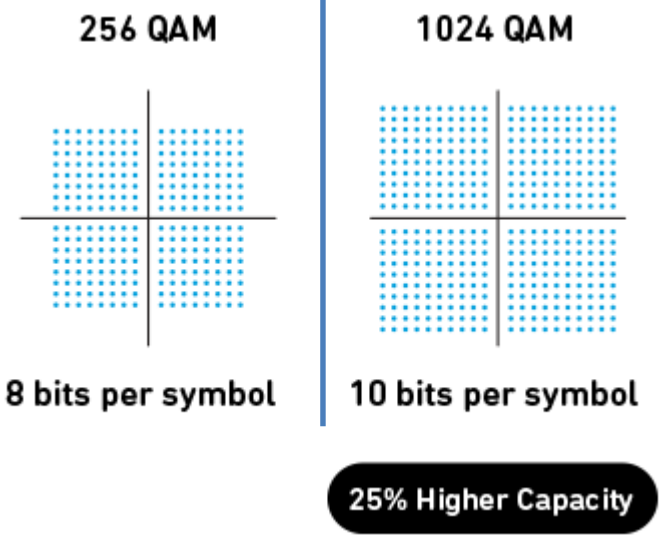
Resource Unit



QAM 調變技術

	802.11ac	802.11ax
BANDS	5 GHz	2.4 GHz and 5 GHz
HIGHEST MODULATION	256-QAM →	**1024-QAM**
DATA RATES	433 Mbps (80 MHz, 1 SS) →	600.4 Mbps (80 MHz, 1 SS)
	6933 Mbps (160 MHz, 8 SS) →	9607.8 Mbps (160 MHz, 8 SS)

Source：ni.com



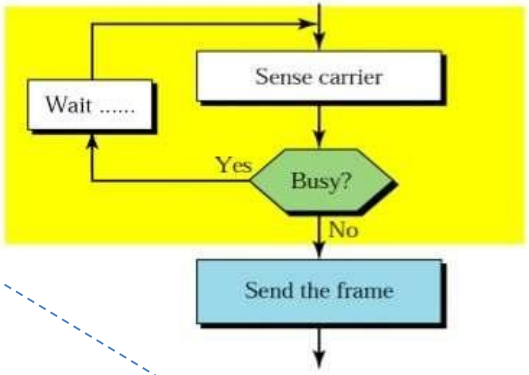
Source：Qorvo

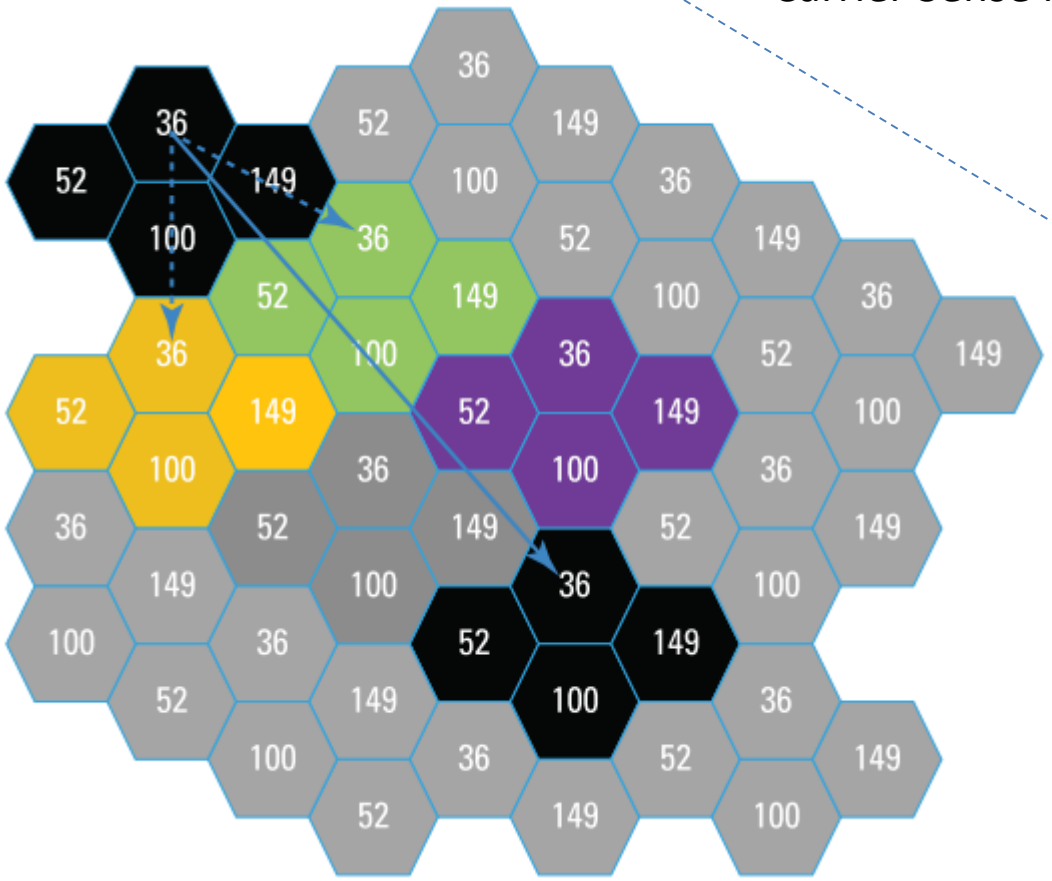
BSS Coloring

CSMA / CA

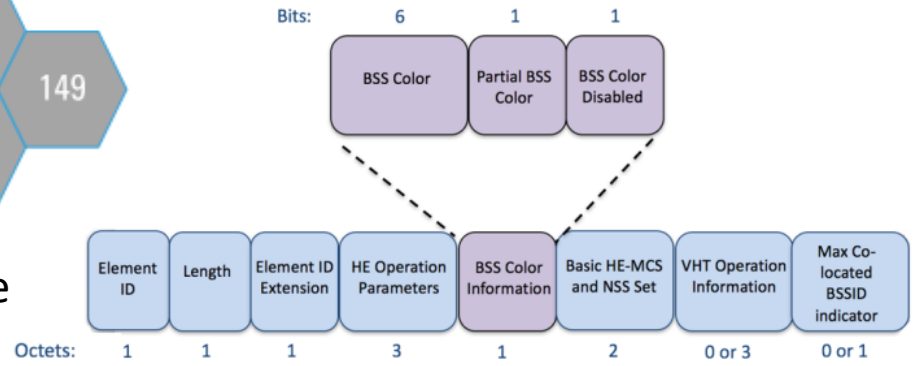
Carrier Sense Multiple Access with Collision Avoidance

Source：rfwireless-world.com





Source：Aerohive



因為行動裝置的極高度普及
無線網路已經是比有線網路
更受使用者使用的上網方式

但是，對於管理者而言
如何提供穩定的服務環境
並且有效控制成本

這都是一大難題

例如：
狀況一 基地台建置地點的選擇，佈建數量的決定
狀況二 該怎樣選擇適當的設備
狀況三 舊技術遇見的瓶頸，新技術提供的解決方式
狀況四 有線網路如何規劃

在本次會議中將會分享

1. 暨南大學的無線網路發展史
2. 挑戰高密度的使用環境
3. 如何提升服務效能
4. 檢討過去的規劃方式
5. 發現高乘載設備的優勢
6. 新技術提供的超能力
7. 優化 5GHz 的方式
8. 安全? 如何做?

報告大綱

- TANetRoaming相關問題詢問
- 暨南大學的無線網路發展史
- 挑戰高密度的使用環境
- 如何提升服務效能
- 檢討過去的規劃方式
- 發現高乘載設備的優勢
- 新技術提供的超能力
- vSZ 可同時支援新舊版本
- 優化 5GHz 的方式

2019/05
TANetRoaming
相關問題詢問

許多使用者會反映未加密的 TANetRoaming SSID會讓其他學校記錄到使用者的明碼帳號與密碼，這一件事情教育部的態度是?

教育部強力推廣EAP-802.1X暨eduroam服務，依漫遊中心與教育部之前開會的討論，後續建置跨校漫遊的部分全面採取，EAP-802.1X驗證，已建置學校也陸續開始進行輔導，當eduroam建置到一定程度後(目前約建置約11%)，會將TANetRoaming服務名稱會修改成iTaiwan (依照校園服務資源對外開放政策)

漫遊中心網頁上提到「請加入漫遊中心的單位於新增或者修改SSID名稱為TANetRoaming」，這邊應該是針對Portal登入的SSID，想要請教的是，除了eduroam之外，有沒有針對802.1x建議的SSID名稱呢?

之前教育部有發函給各連線單位統一SSID為
TANetRoaming(網頁認證)和eduroam(EAP-802.1X)

- TANetRoaming
  - 台灣當初再部署跨校漫遊的部分是採取網頁認證(Web Portal)，為了讓台灣使用者知道哪個SSID可以使用跨校驗證，所以才建議全部都採取TANetRoaming這個名稱
- eduroam
  - eduroam是一個為建立國際教育及科研機構間無線區域網路漫遊體系的計畫。所以外國使用者只會認得eduroam這個名稱。
  - 如校內可以使用802.1X驗證，尊重各校的命名(niu-802.1X、nthu-802.1X等等)，如要開放跨校漫遊就要命名為eduroam，並與漫遊中心完成雙線驗證測試。
  - 另外漫遊中心也強烈建議，未來不管校內校外都統一使用eduroam名稱與國際接軌，漫遊中心也制定了一些使用和設定規範，已減少使用者和建制單位的負擔

2018/06/26公告的訊息Accounting Log一事，請問建議傳送給貴單位的方式，是否由Controller 直接送出? 或是 由syslog Server 進行轉送呢?

Accounting Log主要是因為個連線單位，會因為設備面，政策面或是資安要求的不同，會有儲存相關Log的一些問題，故統一發送到漫遊中心作集中儲存三年，各連線單位就依照自己的需求作相關設定既可。

一般來說Accounting Log都是由Controller直接送出，部分軟體是防火牆可以做到。syslog Server這部分應該都只是記錄自己當下的Accounting Log或是相關紀錄，漫遊中心這邊沒有聽說有這種的運作方式?

暨南大學的無線網路發展史

設備型號	採用規格
Cisco 350	802.11 b
Cisco 1100	802.11 a/b/g
D-Link 2590	802.11 a/b/g/n 2.4GHz or 5GHz

Controller	Aruba Controller Gateway mode

Ruckus 7363	802.11 g/n & n/a 2.4/5 GHz 2×2 : 2 14支天線
Ruckus 7372	802.11 g/n & n/a 2.4/5 GHz 2×2 : 2 12支天線
Ruckus 7982	802.11 g/n & n/a 2.4/5 GHz 3×3 : 3 21支天線

Controller	Ruckus vSCG Controller

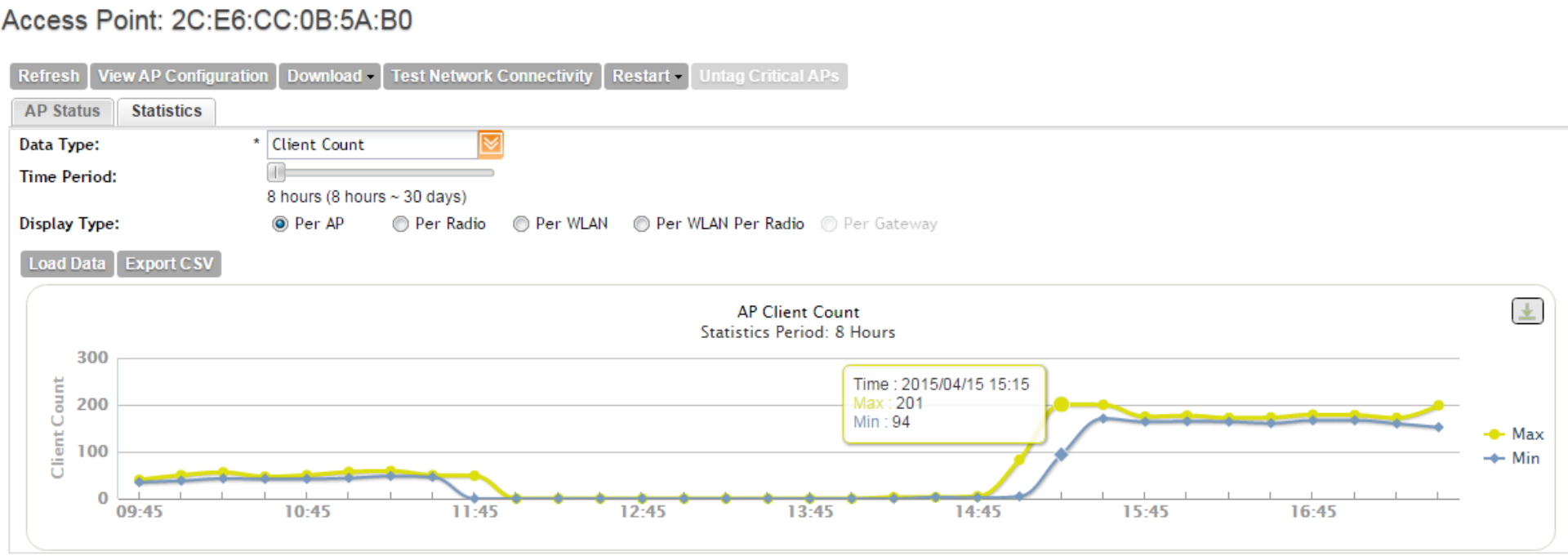
Ruckus R500	802.11 g/n n/a ac 2.4/5 GHz 2×2 : 2 12支天線
Ruckus R600	802.11 g/n n/a ac 2.4/5 GHz 3×3 : 3 12支天線
Ruckus R700	802.11 g/n n/a ac 2.4/5 GHz 3×3 : 3 21支天線
Ruckus R710	802.11 g/n n/a ac 2.4/5 GHz 4×4 : 4 24支天線 wave2
Ruckus T300	802.11 g/n n/a ac 2.4/5 GHz 2×2 : 2

挑戰高密度的使用環境

好幾年前的狀況

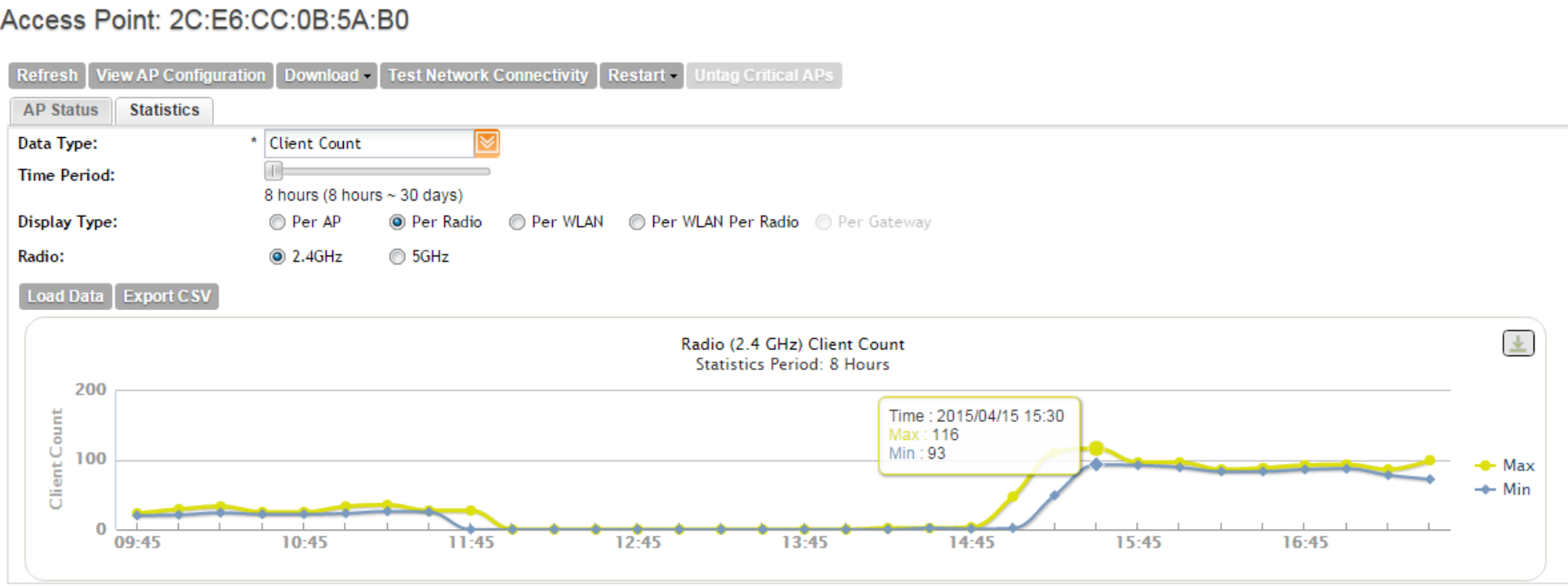
現在正式被肯定

單組 AP 可乘載 201 Client



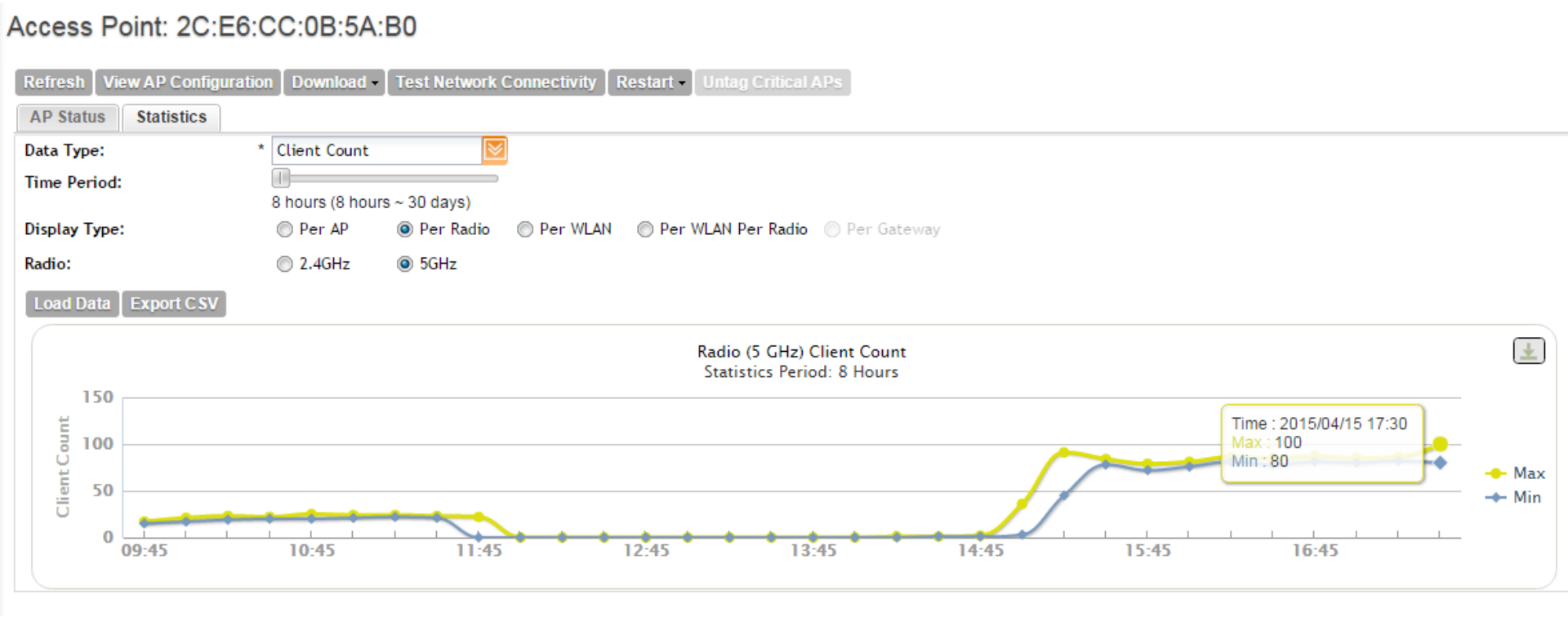
Ruckus 7982

2.4GHz 乘載MAX 116 Client



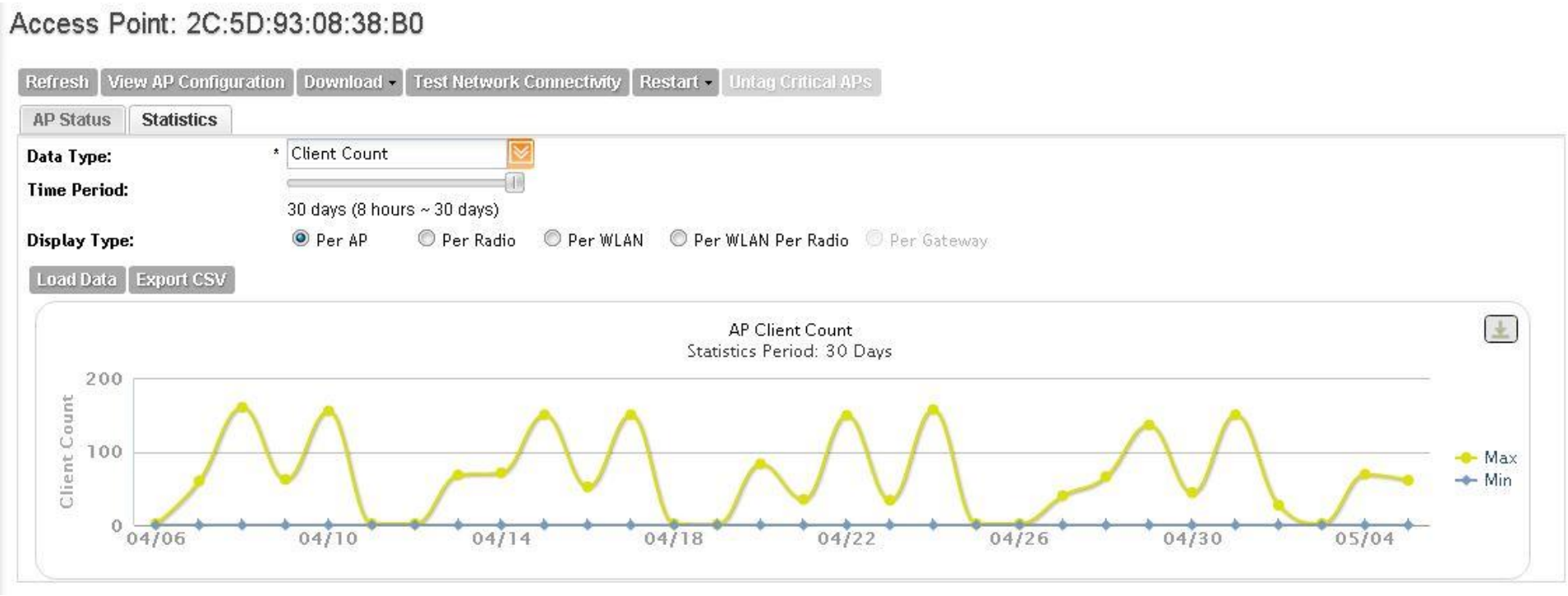
Ruckus 7982

5GHz 乘載MAX 100 Client



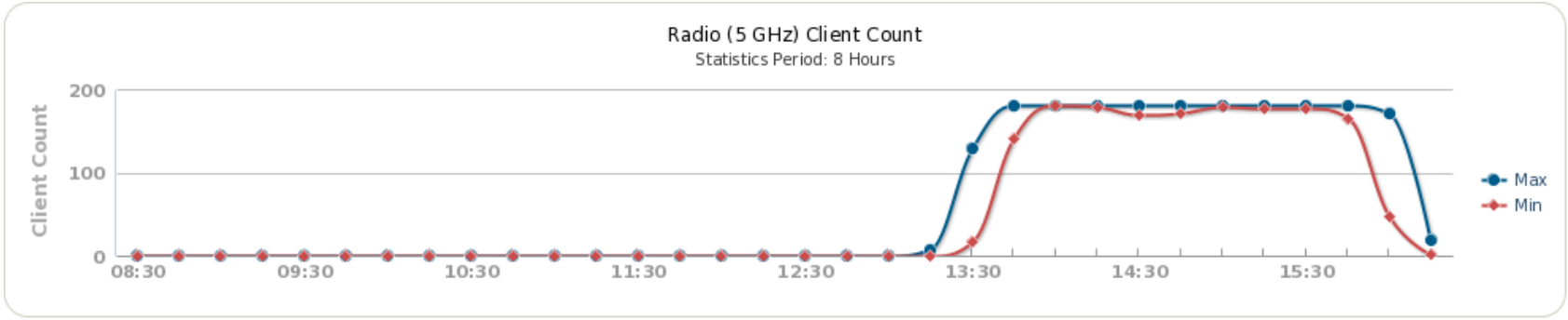
Ruckus 7982

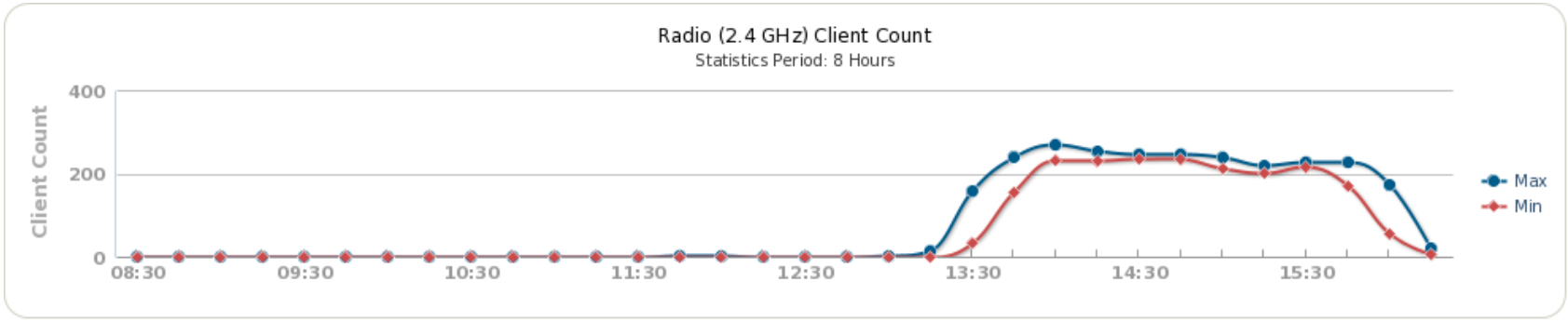
長時間觀察

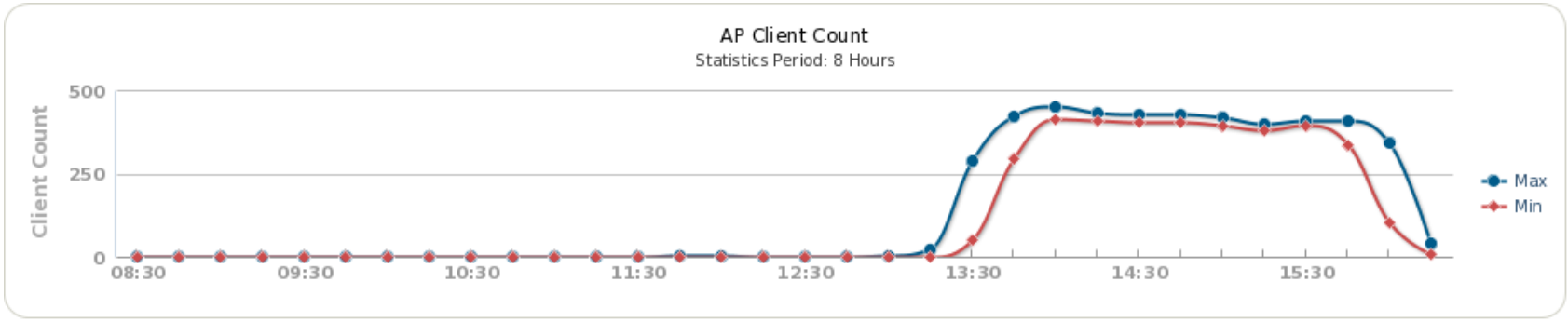


Ruckus 7982

2016/03/16 在校內演講中，記錄到 R500 同時乘載了 449 個 Client
TX 瞬間 最高流量部分也有到 36.7 Mbps


Radio (5 GHz) Client Count
Statistics Period: 8 Hours
Client Count
200
100
0
08:30
09:30
10:30
11:30
12:30
13:30
14:30
15:30
Max
Min


Radio (2.4 GHz) Client Count
Statistics Period: 8 Hours
Client Count
400
200
0
08:30
09:30
10:30
11:30
12:30
13:30
14:30
15:30
Max
Min


AP Client Count
Statistics Period: 8 Hours
Client Count
500
250
0
08:30
09:30
10:30
11:30
12:30
13:30
14:30
15:30
Max
Min

如何提升服務效能

其實並不困難

管理者 所需要了解的資訊

1. 測量空間中訊號衰減狀況
2. 空間內須提供服務的設備數量上限
3. 依環境推估使用者可能使用的設備類型
4. 尋找適當的設備

檢討過去規劃的方式

挑戰備援機制 與 分流問題

早期的建置方式：

1. 採用多組無線網路基地台
2. 單台設備成本便宜
3. 分流使用者的流量
4. 提供備援機制

Site Survey– 新舊測試報告

發現的瓶頸：

1. 大量建置導致 2.4GHz同頻段干擾相當嚴重
2. 有形成本 – 設備與線路
3. 無形成本 – 管理與人力

消失的成本

發現高乘載設備的優勢

成本試算 – 每人平均成本

- 若是教室內有 50個 座位
- 推估 設備量為人數之兩倍，約為 100 個

單台AP的乘載量	AP單價	所需數量	AP成本	單一連線成本
35人	6,000元	最少三組	18,000元	180元
120人	12,000元	只需一組	12,000元	120元

總成本試算

20間教室，每間50個座位，設備量為人數之兩倍

AP類型	AP數量	實體線路	24 Port PoE Switch	License
低乘載	60台	60條	3 台	60組
高乘載	20台	20條	1台	20組

迷思

- –分流機制
- –備援機制

當 AP 當機時，備援組無法收納所有使用者的連線，無線服務依舊停擺

發現新技術的超能力

解決舊技術遇見的瓶頸

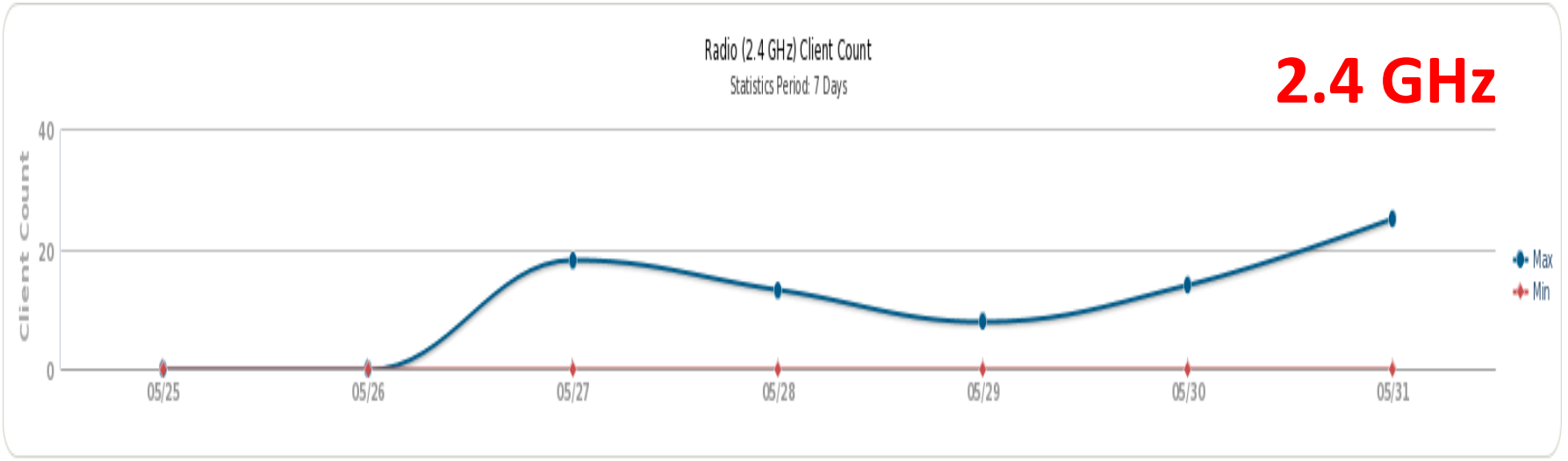
不同頻段 - 分流概念

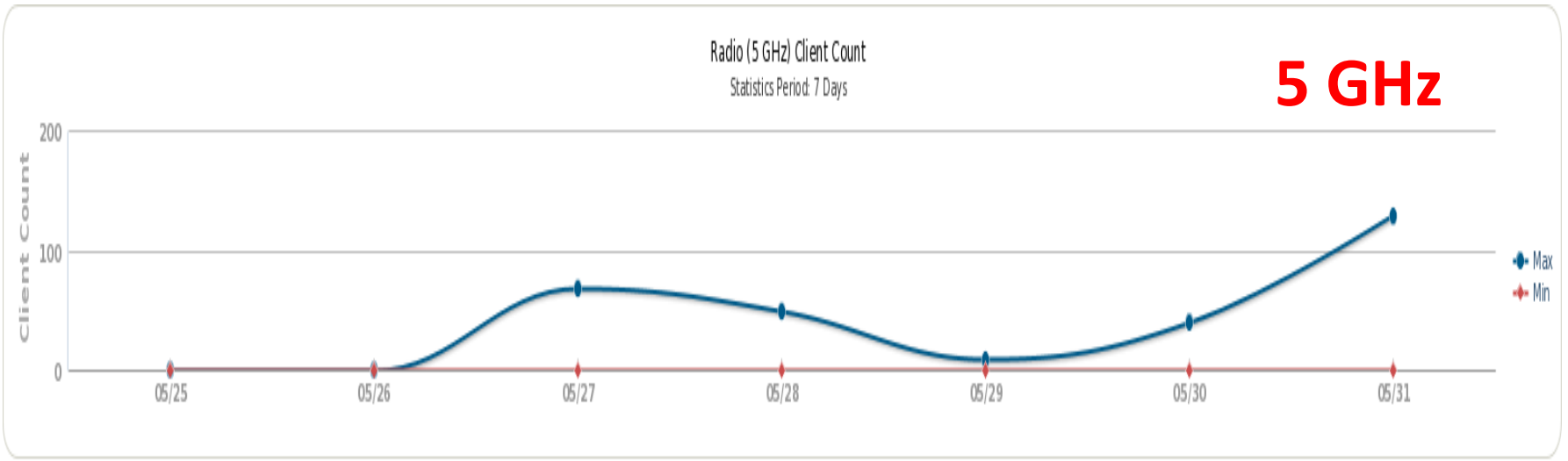
正視 5GHz 的使用者快速增加
透過 Dual band 的方式分流 2.4GHz & 5GHz的 Client
一台高乘載的 Ruckus AP 當兩台使用

Access Point: 2C:5D:93:08:38:B0

Radio 802.11g/n		Radio 802.11a/n	
Current Channel	11	Current Channel	153
Channelization	20MHz	Channelization	40MHz
WLAN Group	default	WLAN Group	default
Background Scan	Disabled	Background Scan	Enabled
TX Power	Full	TX Power	Full
# of Authorized Clients	72	# of Authorized Clients	45

2019/05/31 - 5GHz 已經超越 2.4GHz





如何挑選頻道

- 同頻干擾的嚴重性

  眼睛看得到，Ping 值高達 300~500

- 演算法

  依據不同 Channel 的可用頻寬

  自動挑選適當的 AP Channel

智慧型天線（Smart Antenna）

智慧型天線（Smart Antenna）的發展來自於適應性天線陣列（Adaptive Antenna Array）

增加天線增益（Antenna Gain）提升訊號雜訊比（SNR；Siganl to Noise Ratio），有利於雜訊的消除。

並且降低多路徑衰落（multipath fading）與時間延遲延展（time delay spread），以及增加發射效率（transmission efficiency）與訊號涵蓋範圍。

波束成型技術（BeamForming）

必須同時結合晶片、天線以及軟體控制

才能發會最好的效果，IEEE802.11ac，已經將Beamforming標準化

256 QAM調變技術

正交振幅調變技術的改變
(QAM；Quadrature Amplitude Modulation)

IEEE 802.11n標準採用的是64 QAM
IEEE 802.11ac的標準中已經提升採用256 QAM

指一個封包可以乘載的資料量多寡
直接的影響是傳輸速率的改變

多重輸入與輸出 MIMO
(Multi-input Multi-output)

T x R : S

發射天線數量 X接收天線數量：空間流數

3 x 3 ： 3 說明的是

三支發射天線與三支接收天線提供三個空間流

4 x 4 ： 3 代表有一組天線是冗餘收發器

802.11ac
802.11ax (Wi-Fi6)

	802.11ac	802.11ax
BANDS	5 GHz	**2.4 GHz** and 5 GHz
CHANNEL BANDWIDTH	20 MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz	20 MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz
FFT SIZES	64, 128, 256, 512	256, 512, 1024, 2048
SUBCARRIER SPACING	312.5 kHz	**78.125 kHz**
OFDM SYMBOL DURATION	3.2 us + 0.8/0.4 us CP	**12.8 us + 0.8/1.6/3.2 us CP**
HIGHEST MODULATION	256-QAM	**1024-QAM**
DATA RATES	433 Mbps (80 MHz, 1 SS) 6933 Mbps (160 MHz, 8 SS)	600.4 Mbps (80 MHz, 1 SS) 9607.8 Mbps (160 MHz, 8 SS)

資料來源 http://technews.tw/2017/09/20/qualcomm-802-11ax-wi-fi/

優化 5GHz 的方式

有效提升使用感受
如何讓使用者優先使用

各校常見的發展過程

早期　Tunnel - Single Point of Failure

改善　New Topology

進化　Trunk – Native Vlan

Tunnel - SPOF

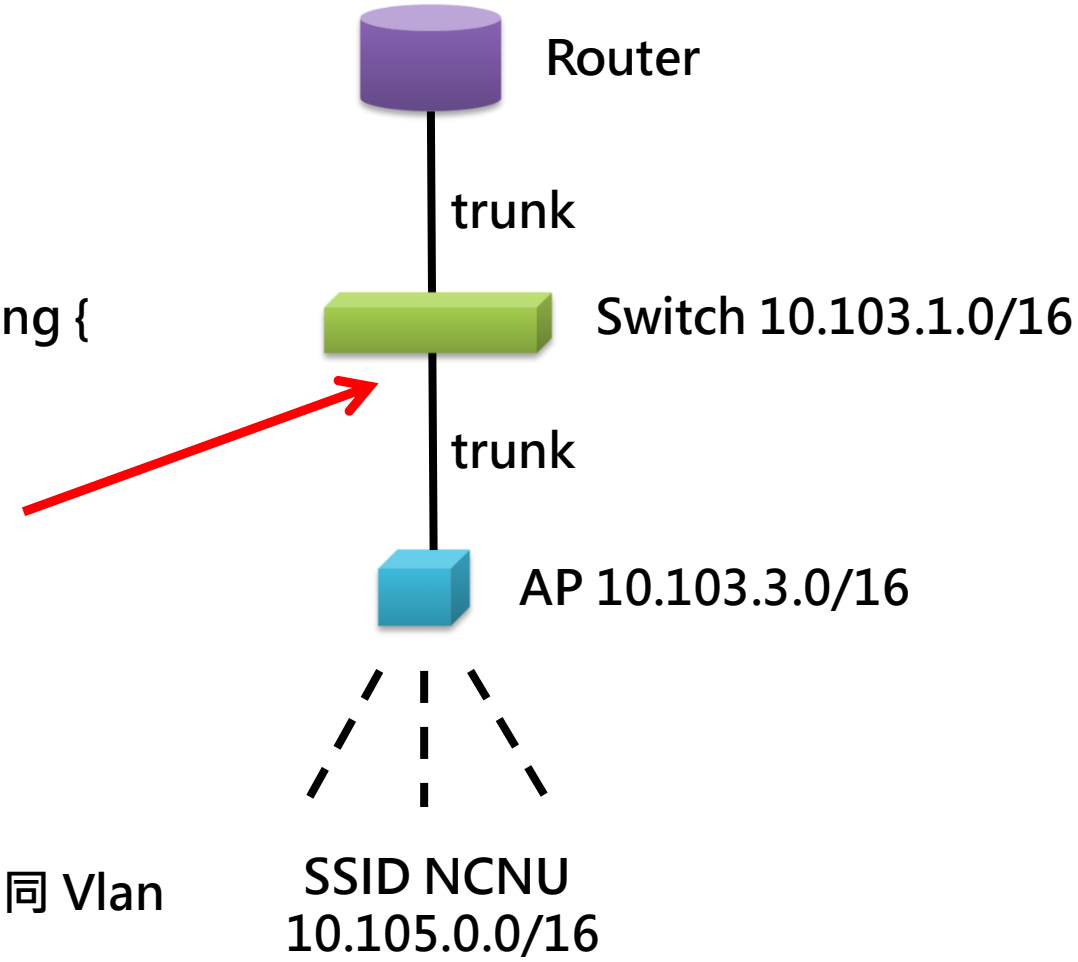
- 當所有流量都回到 Controller
  - 早期使用量不多時可能不成問題，但是當loading增加時，管理者的心臟就要越大顆
- 當使用者越多時
  - 加密傳輸是一種可能造成設備負載的狀況，尤其當原本拓樸上有異常狀況發生時，可能開始有接不完的抱怨電話

New Topology

- 早期現象
  - 使用 Tunnel mode 易於建置，經常將AP建置在原本的實體線路上
- New Topology 易於查修
  - 無線網路查修較為困難，因此為了便於查修，常見的做法是佈建實體線路，提供 一張新的網供無線網路服務
- 實際案例
  - 備援機制 – 學校又停電了，但是無線網路是通的
  - 業務權責 – 管理和問題查修上，有利於確判別問題

Trunk – Native Vlan

```
interfaces {
   ge-0/0/0 {
      unit 0 {
         family ethernet-switching {
            port-mode trunk;
            vlan {
               members v105;
            }
            native-vlan-id v103;
         }
      }
   }
```



讓 management 與data分在不同 Vlan
避免廣播封包造成管理上的問題

最在乎的報表資訊

- 那些 AP 遇到同時上線的 Client 接近危險邊緣
  - 建議：是否需要增加AP
- 那些 AP 下的使用者連線訊號最糟糕
  - 建議：調整AP位置或增加AP

各項經驗總結

- 人在哪、基地台就安裝在哪
- 選擇支援智慧型天線的必要性
- 有線網段的規劃與設計

無線網路安全嗎?

2015
https://news.tvbs.com.tw/life/615399

2018
https://news.tvbs.com.tw/world/892678

在暨南大學上網不用認證?

SSID：NCNU 安全性問題

全校各區數量

男研 1台
女研 1台
男宿 1台
女宿 1台
餐廳 3台
體健中心 6台
活動中心 17台

圖資 29台
管院 50台

行政 24台
教A　24台
教B　10台
人院 47台
汙水　1台

科一館 15台
科二館 26台
科三館 22台
科四館 23台
地震所　2台
學人會館 8台
校長宿舍 2台
前主任家 1台

台中育成 2台
香港 1台

目前全校AP類型與數量

全部支援 2.4G/5G Dual band，共計317台
依照使用區域內的不同程度的需求，佈建不同等級的AP

802.11ac wave2
R710　17台

802.11ac wave1
T300　1台
R700　2台
R600　2台
R310　12台

802.11n
R500　99台
R7982 8台
R7372 103台
R7363 73台

所有使用的 SSID

NCNU

NCNU - Activity Center

NCNU - Restaurant

NCNU - Sports

NCNU-CC

NCNU-EMBA

NCNU - HK

NCNU-President

TANetRoaming (iTaiwan)

eduroam

既有法規

無線網路環境使用者身份認證機制

100年6月21日99學年度計算機與網路中心諮詢委員會第2次會議通過

中華民國100年9月21日 國立暨南國際大學（100）暨校電字1000011674 號函公佈實施

依據：為配合臺灣學術網路政策，進行資訊安全層級提升，建置無線網路環境使用者身份認證機制，貫徹本校無線網路環境下資訊安全與使用權限控管

施行細則

說明：

- 未來校園內，欲使用學校所提供之無線網路，均需經過認證。
- 認證帳號為本校email 帳號(不需輸入 @ncnu.edu.tw)。
- 他校訪客亦可透過「TANet 無線網路漫遊服務」利用他自己學校的帳號認證。
- 本校的教職員工生，若已在教務系統內填寫您的網路卡卡號，則無須每次連上無線
- 網路時輸入帳號密碼進行認證。
- 無以上登入方式之訪客，可由邀請單位建立臨時帳號。

資安問題

- 無線網路身份確認
  - 是否列為ISMS的管控項目，請共同討論

    NCNU-ISMS-B-007-通信與作業管理程序書

    5.5.3無線網路使用之管理
    5.5.3.1無線網路基地台之使用應有適當控管。
    5.5.3.2內部無線網路之使用應取得授權，禁止於內部網路私自使用未經授權之無線網路產品。
    5.5.3.3無線網路設備之使用應有適當管理紀錄，例如：授權使用之IP位址、連接埠、網卡位址（MAC）等。
    5.5.3.4無線網路之資料傳輸宜使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。

- 法規是否合宜
  - 無線網路環境使用者身份認證機制法規是否符合現行環境，請共同討論

提升資安層級目標

中興大學
身份認證 無校園法源依據，主要是為了能找到人

中央大學
身份認證 無校園法源依據，主要是為了能找到人

交通大學
身份認證 無校園法源依據，主要是為了能找到人
不給校外人士使用TANet，提供 Hinet給校外使用者連線使用

台灣大學
身份認證+連線加密，無校園法源依據，主要是為了能找到人

各校共同目標

要找到人

以下彙整四種方式

方法一 網卡認證

- 操作模式
  - 先在教務系統登記網路卡卡號
- 便利性
  - 連上線後可以直接使用
- 困難點
  - 同一台設備在不同時期由不同人使用，可能無法正確找到使用者，例如共用的筆電或是平板
  - 登錄資料更新是週期性的，不會馬上登記馬上生效

方法二 網頁認證

- 操作模式
  - 連線後由認證網頁輸入 E-mail 帳密
- 便利性

  由於不斷要輸入帳密，所以不方便
- 困難點
  - 對於行動裝置較小銀幕輸入不便
  - 離線後一段時間若要再使用，則需重複輸入帳密
  - 登入畫面不一定每一次都會彈掉

方法二 網頁認證


國立暨南國際大學 - 無線
不安全 | 163.22.3.15:9997/SubscriberPortal/?nbiIP=163.22.12.125&client_mac=ENCbc22268ef4c0446ab9a2fa79cd6ec3bf7a8dbb9754dde0ab&sip=scg.ruckuswirel...
教育部 Ministry of Education
無線網路帳號認證系統
登入系統 Login to the system
請使用「漫遊帳號」登入本系統
使用注意事項
1. 使用者應尊重智慧財產權。
2. 使用者禁止濫用網路資源。
3. 應注意網路隱私權之保護。
4. 使用者需遵循校園網路使用規範。
5. 請使用您"來賓帳號"登入本系統。
6. 服務時間：每日AM6:30~PM24:00。
查看詳細校園網路使用規範
如需協助請洽 77365795、77365796
National Chi Nan University
Wireless Authentication Portal
Type TANet
User Name 請輸入帳號
Password 請輸入密碼
Sign In

方法二 網頁認證

手機操作畫面

方法三 802.1x認證

- 操作模式
  - 連線AP時就會要求輸入 E-MAIL 帳密
  - 802.1x
- 便利性
  - 設備只需要第一次進行認證，之後連線就不需認證
- 困難點
  - 第一次登入時必須做額外設定
  - 同一台設備在不同時期由不同人使用，可能無法正確找到使用者，例如共用的筆電或是平板

方法三 802.1x認證

額外設定說明

1. Apple行動裝置
2. Android 行動裝置
3. Windows 10 作業系統
4. Windows 7 作業系統

方法四 安裝Agent

- 操作模式
  - 安裝agent
- 便利性
  - 安裝一次後，就可以不用再輸入帳密並自動連線，可限制使用權限
  - 安全性最高
- 困難點
  - 費用很高

討論各項問題

方法二 認證網頁問題

- 為了攔截封包觸發開啟認證畫面
  - 版本1：所有流量會過 Controller
    - 優點：一定會跳出網頁認證畫面
    - 問題：Controller 比較忙碌
    - 流量平均高峰值500Mbps
    - 需額外加買授權
  - 版本2：使用者流量不經過 Controller
    - 問題：認證畫面有可能沒跳出來
    - 優點：Controller 不會變成瓶頸
    - 預計在03/01 進行升版測試

網卡+網頁認證 混合作法

- 暨大早期
  - 如果有網卡認證即可上網，若無網卡認證則由網頁認證
- 交大
  - 網頁認證登入後，將設備的網卡轉至網卡認證模式，但若太久沒有使用清掉網卡資訊，可以保持長時間不用輸入帳密進行身份確認

連線加密問題

- 僅作身份認證確實可以 找到人
- 資工系教授表示 連線不安全

- 解決辦法為採用
  - 方法三 802.1x認證
    - 提供不同作業系統的登入教學
    - http://wlan-roaming.ncnu.edu.tw/eduroam.html
  - 方法四 安裝Agent
    - 這需要花很多很多錢向廠商買授權

需登入帳密方式比較

- 方法二 網頁認證
  - 網頁認證需要不斷重複登入
  - 離線後最長xxx秒會timeout
  - 不一定會跳出網頁問題

- 方法三 802.1x認證
  - 只需要登入過一次就不用再輸入
  - 除了APPLE裝置外，其他設備第一次連線之前需要稍作設定

目前的 SSID 以及 安全性

- NCNU 系列
  - 無身份認證
  - 無連線加密
- TANetRoaming(iTaiwan)
  - 方法二 網頁認證
  - 有身份認證
  - 無連線加密
- eduroam
  - 方法三 802.1x 認證
  - 有身份認證
  - 有連線加密

臺灣學術網路(TANet)技術小組第88次會議

時間：103年4月22日(星期二)下午2時30分　網址

討論事項

案由一、有關TANet與iTaiwan雙向漫遊開放互連相關事宜，提請討論。

決議：

(一) 為使現在及未來開放之無線網路服務能有標準規範及有效運作，本部將召集相關人員研擬制定校園無線網路服務漫遊管理規範。

(二) 為求各校與iTaiwan雙向漫遊認證登入頁面統一，請臺灣學術網路漫遊中心(宜蘭大學)於本年5月31日前完製登入頁面範例，以供各區網及縣市網路中心參考使用。

(三) 請各區網中心考量於今年6月底前完成雙向漫遊認證登入頁面建置作業，並於無線漫遊認證登入頁面中加入「iTaiwan」身份選項或加註文字說明（帳號加上@itw即可(例:0936609881@itw)）。

(四) 為配合Eduroam國際漫遊聯盟SSID命名規範，以利國外學者辨識並使用校園無線網路，建請TANet無線網路漫遊機制之各校(或機關構)考量增設一組SSID：eduroam。

(五) 對各國中小學校校園開放雙向漫遊服務，請縣(市)網路中心先依實際所能提供之服務能量及需求，在不影響學校教學之原則下，研訂於校園提供無網路漫遊服務點(AP)的數量及開放時間，並協助提供資科司可漫遊之服務點位置及數量。

推廣期的作法

- 即日起至 107/07/31
- 學校首頁貼公告
  - http://wlan-roaming.ncnu.edu.tw
- 發公文至各單位
  - http://wlan-roaming.ncnu.edu.tw
- 教育訓練
  - 新生訓練座談與新生手冊

推廣期間

- 針對推廣期間問題討論
  - 對於沒有認證和連線加密的SSID的處理方式
  - 新 SSID 名稱和安全機制
  - 討論是否保留既有兩組 SSID
    - TANetRoaming(iTaiwan)
    - Eduroam

討論方案一

- 提供討論的方案一
  - 推廣期間保留 NCNU、TANetRoaming(iTaiwan) 和 eduroam
  - 新增一系列 NCNU-區域名稱 具安全機制的SSID

    例如....
    - NCNU - AA (行政大樓)
    - NCNU - LC (圖資大樓)
  - 已經帶有NCNU-區域名稱的SSID直接改成需要認證
    - NCNU - Activity Center
    - NCNU - Restaurant
    - NCNU - Sports
    - NCNU - CC
  - 推廣期間之後移除 NCNU

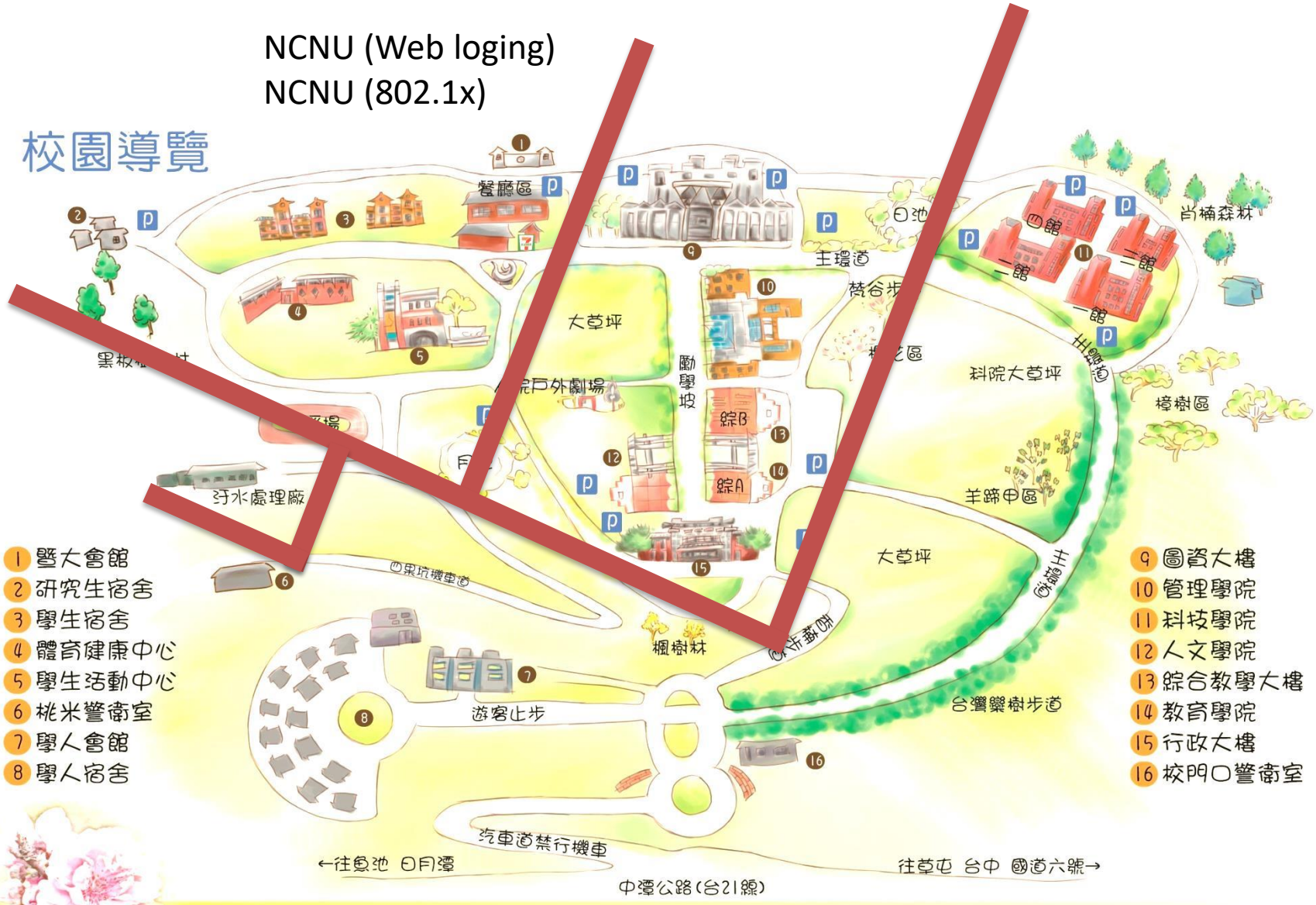
- 預期目標
  - 提升安全性
  - 附加價值：可將網段縮小，降低廣播範圍，提升服務品質

討論方案二

- 簡化 SSID
- 全校統一使用兩組SSID
  - NCNU (Web Loging)
  - NCNU (802.1X)

- 縮小廣播範圍 /20 可用 IP address 約為4096
  - 科院區 (科一、科二、科三、科四)
    - Native 103
    - NCNU (Web Loging) 104
    - NCNU (802.1x) 105
  - 中軸區 (圖資、管院、教學A、教學B、人院、行政)
    - Native 106
    - NCNU (Web Loging) 107
    - NCNU (802.1x) 108
  - 餐廳宿舍 (包含 體健中心、學生活動中心)
    - Native 130
    - NCNU (Web Loging) 131
    - NCNU (802.1x) 132
  - 學人會館區
    - Native 133
    - NCNU (Web Loging) 134
    - NCNU (802.1x) 135

NCNU (Web loging)
NCNU (802.1x)



National Chi Nan University

觀察與統計

統計項目

1. SSID 的連線統計 NCNU、TANetRoaming(iTaiwan)、eduroam
2. AP的使用統計 (AA、HA、CA、CB....)
3. 作業系統統計 (IOS、Android...)
4. 加密機制統計 (WPA2-AES、None)
5. Radio 統計 ([a/n/ac]、[g/n]、[a/n])

組合

x (y1、y2、y3.....yn)

加入時間軸繪圖

宿舍區 WIFI

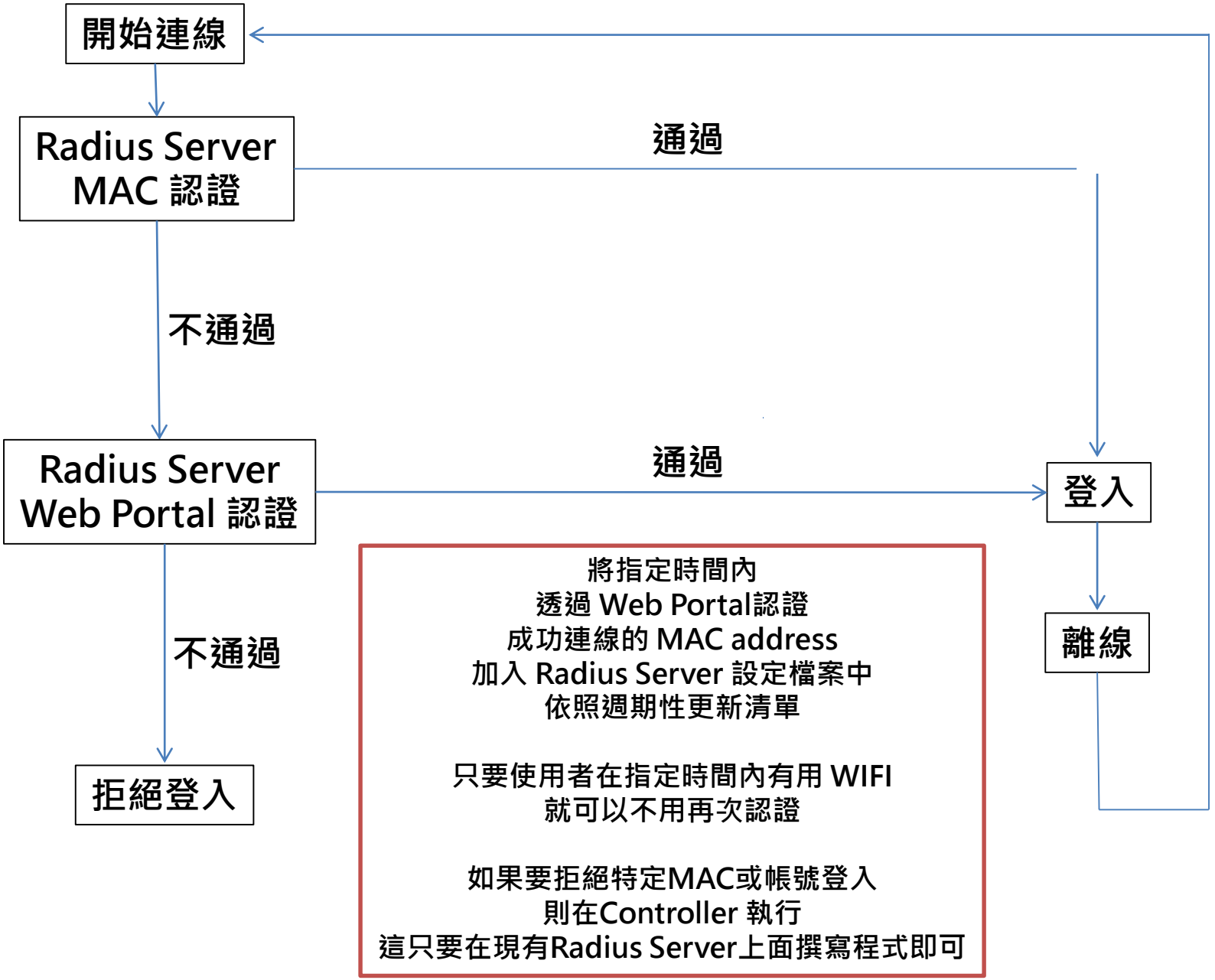
- 大學部
  - 女生宿舍
    - 65台 AP
    - 4台 PoE Switch
    - 配線
  - 男生宿舍
    - 65台 AP
    - 4台 PoE Switch
    - 配線
- 研究生
  - 不建議安裝
    - 因為裝在走廊傳輸訊號不佳，因為防火門造成訊號衰減太大
    - 裝在房間內幾乎是在同學的床邊，感官不佳
    - 裝在房間內難以保管

如何建置
802.1x 無線網路認證

暨大怎麼做?

怎麼讓使用者
不需要一直打帳密

暨大怎麼做?


開始連線
Radius Server
MAC 認證
通過
不通過
Radius Server
Web Portal 認證
通過
登入
不通過
離線
拒絕登入
將指定時間內
透過 Web Portal認證
成功連線的 MAC address
加入 Radius Server 設定檔案中
依照週期性更新清單
只要使用者在指定時間內有用 WIFI
就可以不用再次認證
如果要拒絕特定MAC或帳號登入
則在Controller 執行
這只要在現有Radius Server上面撰寫程式即可

順利登入的 LOG 範本

Sun Aug 19 00:50:43 2018 : Auth: Login OK: [ycc/password] (from client MAC-LOGIN port 0 cli E4-70-B8-33-2F-EA)

Sun Aug 19 00:51:41 2018 : Auth: Login OK: [80656DABCDEF/80656DABCDEF] (from client MAC-LOGIN port 0 cli 80-65-6D-AB-CD-EF)

IOT 設備怎麼辦

- 手動將 MAC 加入 Radius
  - 被動加入
  - 系統申請方式
  - 有其必要性

經驗分享

感謝您的參與