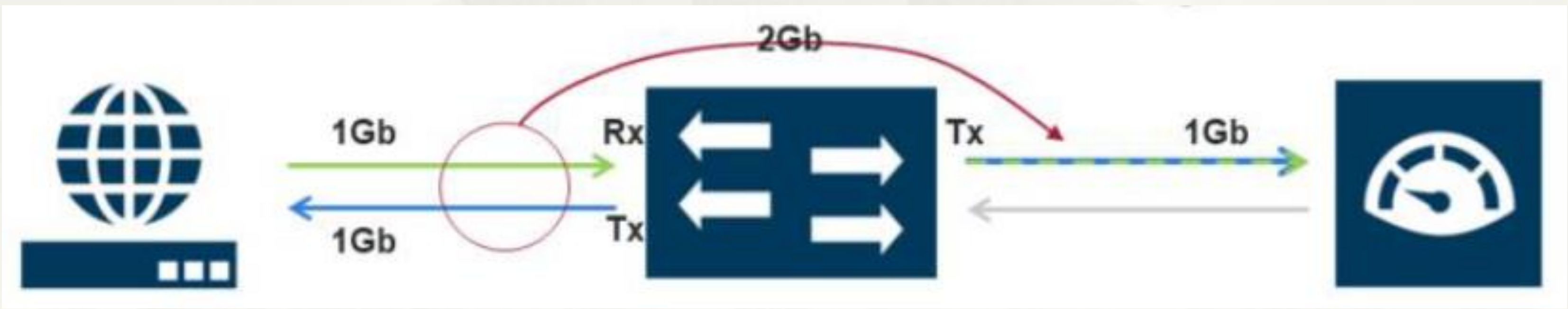
頻寬分流管理器
Inline Bypass Mirror
架構簡介

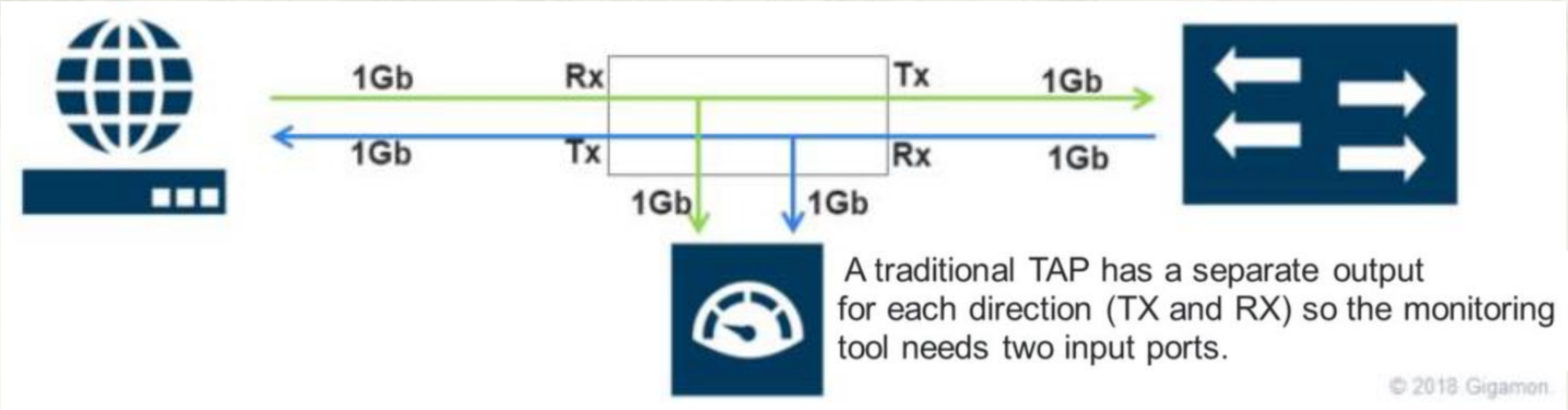
臺灣大學計資中心
游子興
davisyou@ntu.edu.tw
3366-5008

Mirror vs. TAP

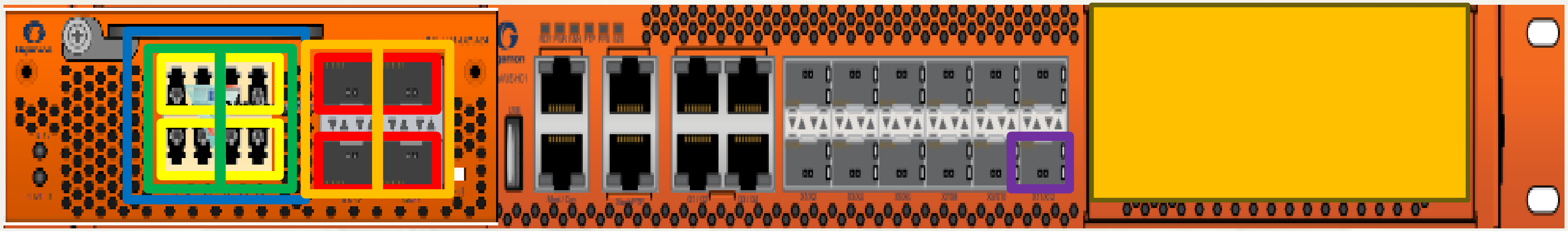
- SPAN/Mirror



- TAP



Gigamon HC1

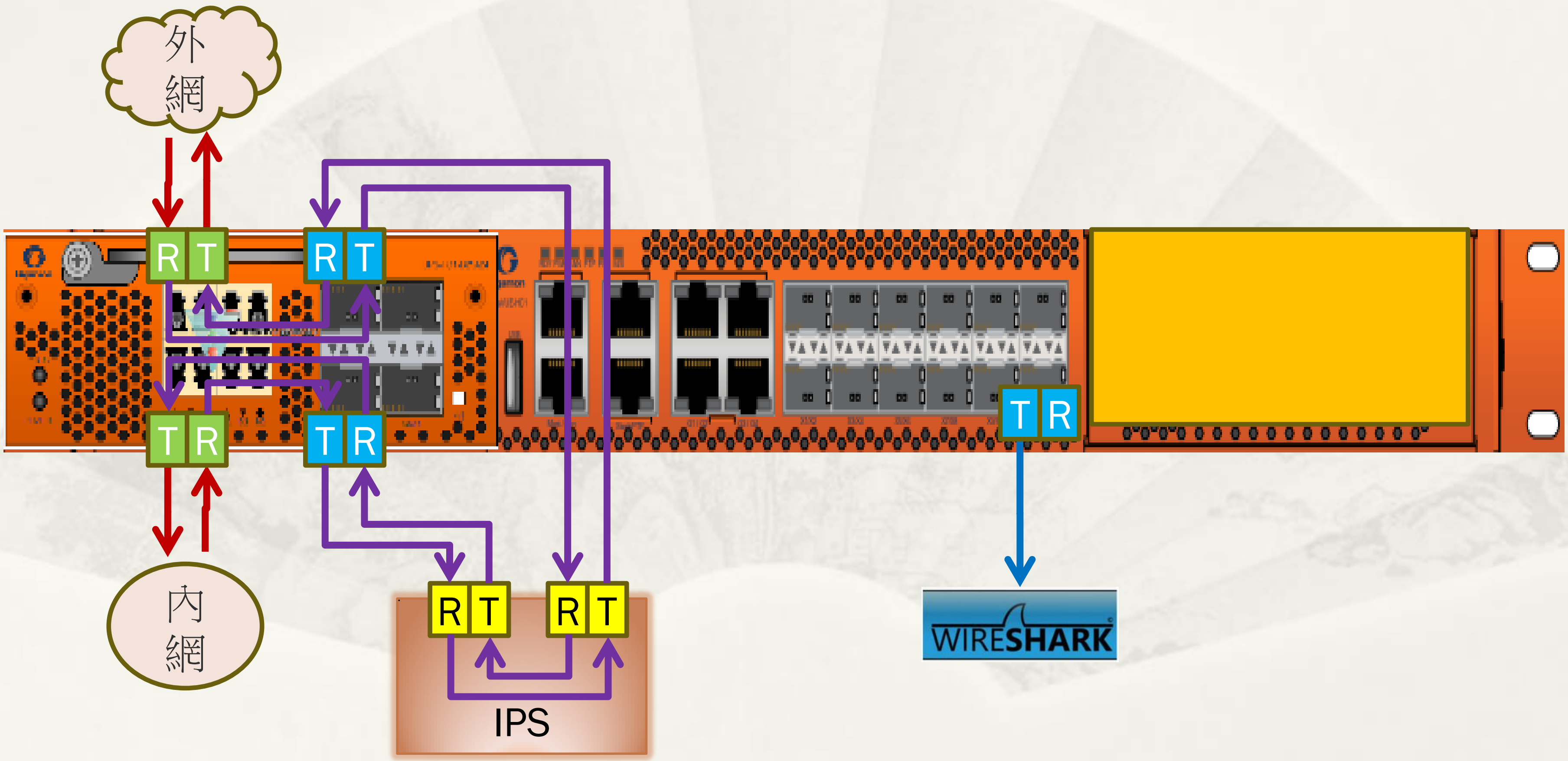


Inline Network Port
Inline Network
Inline Network Group

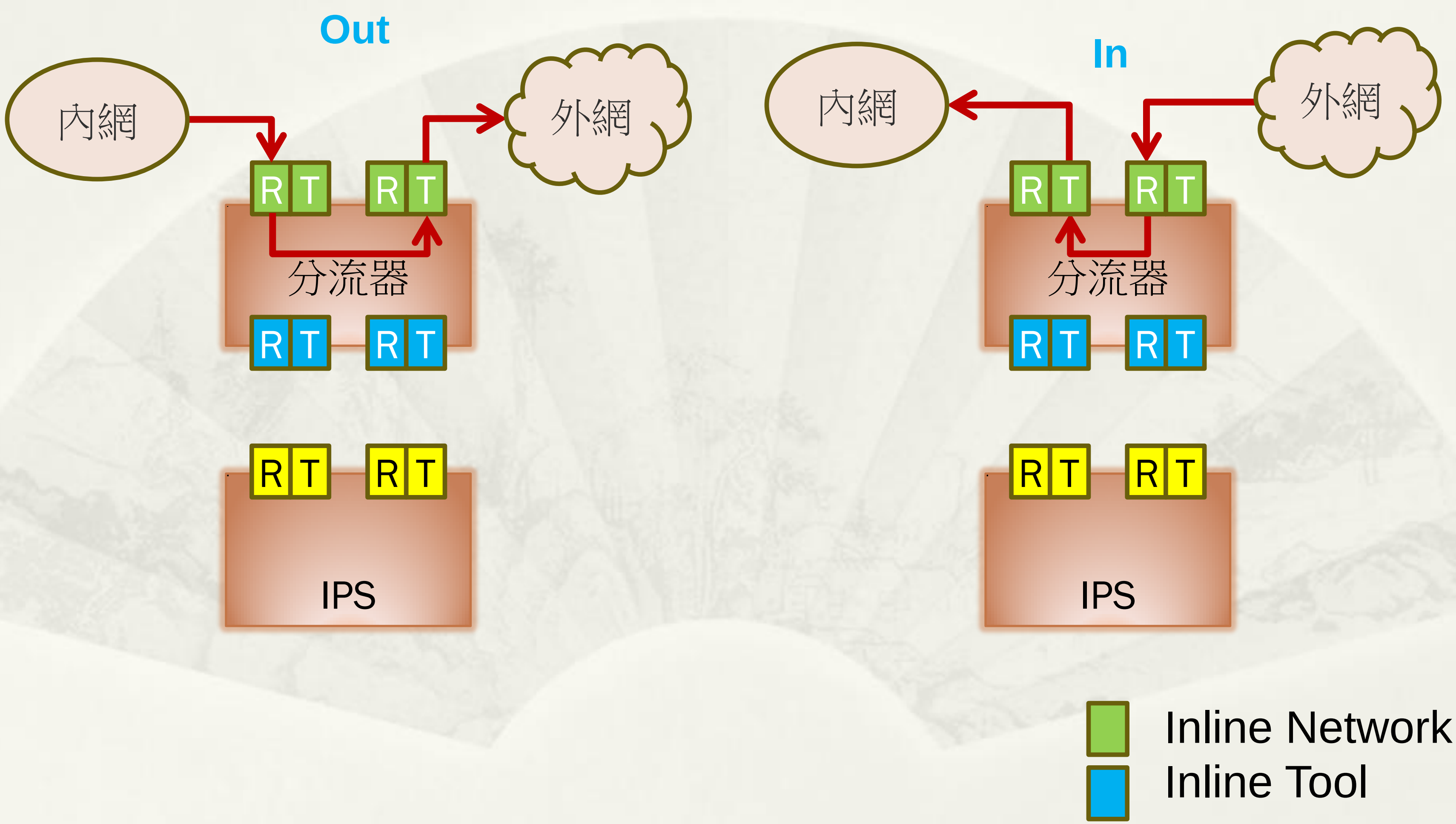
Inline Tool Port
Inline Tool

Tool Port

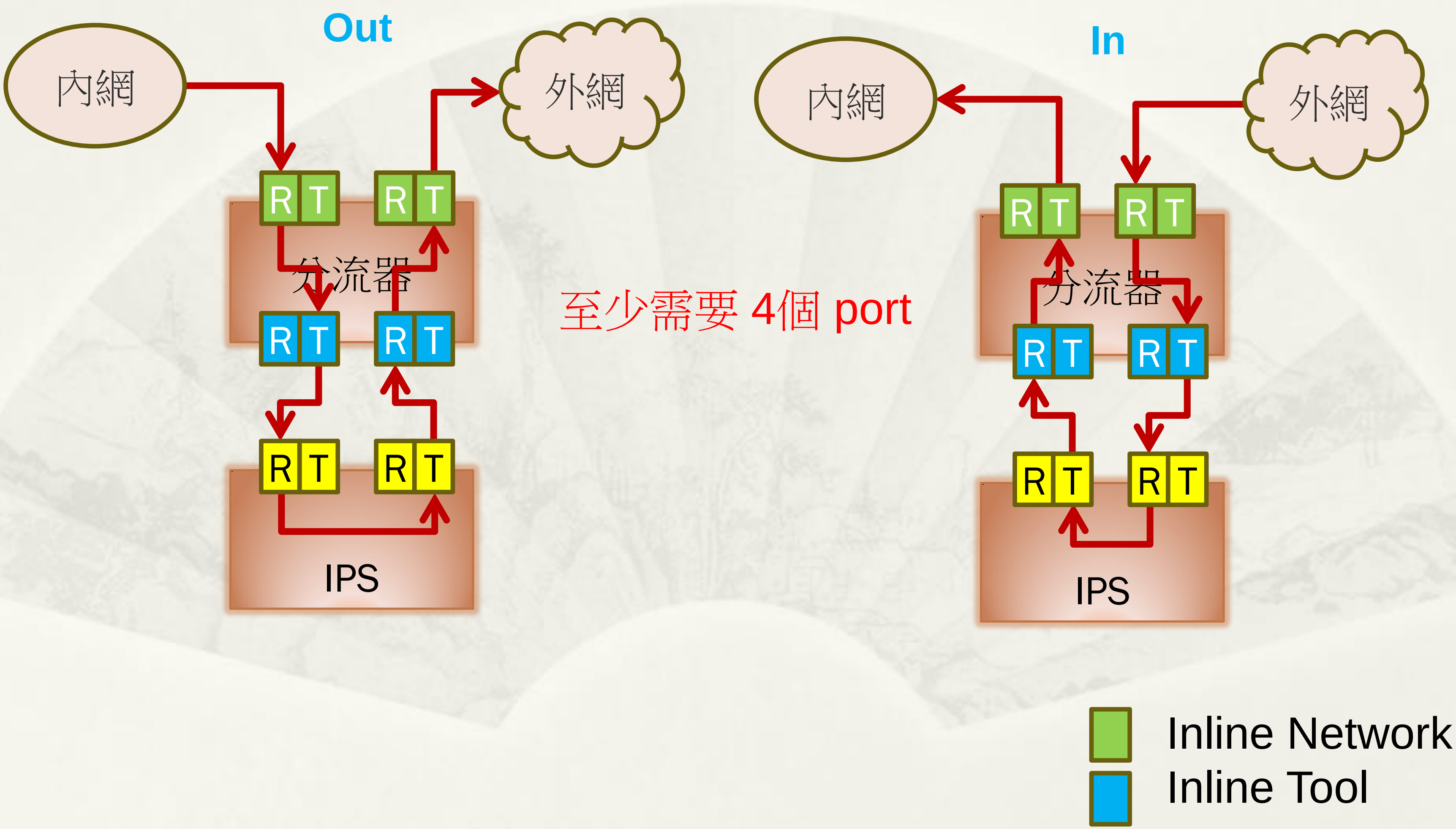
Gigamon HC1



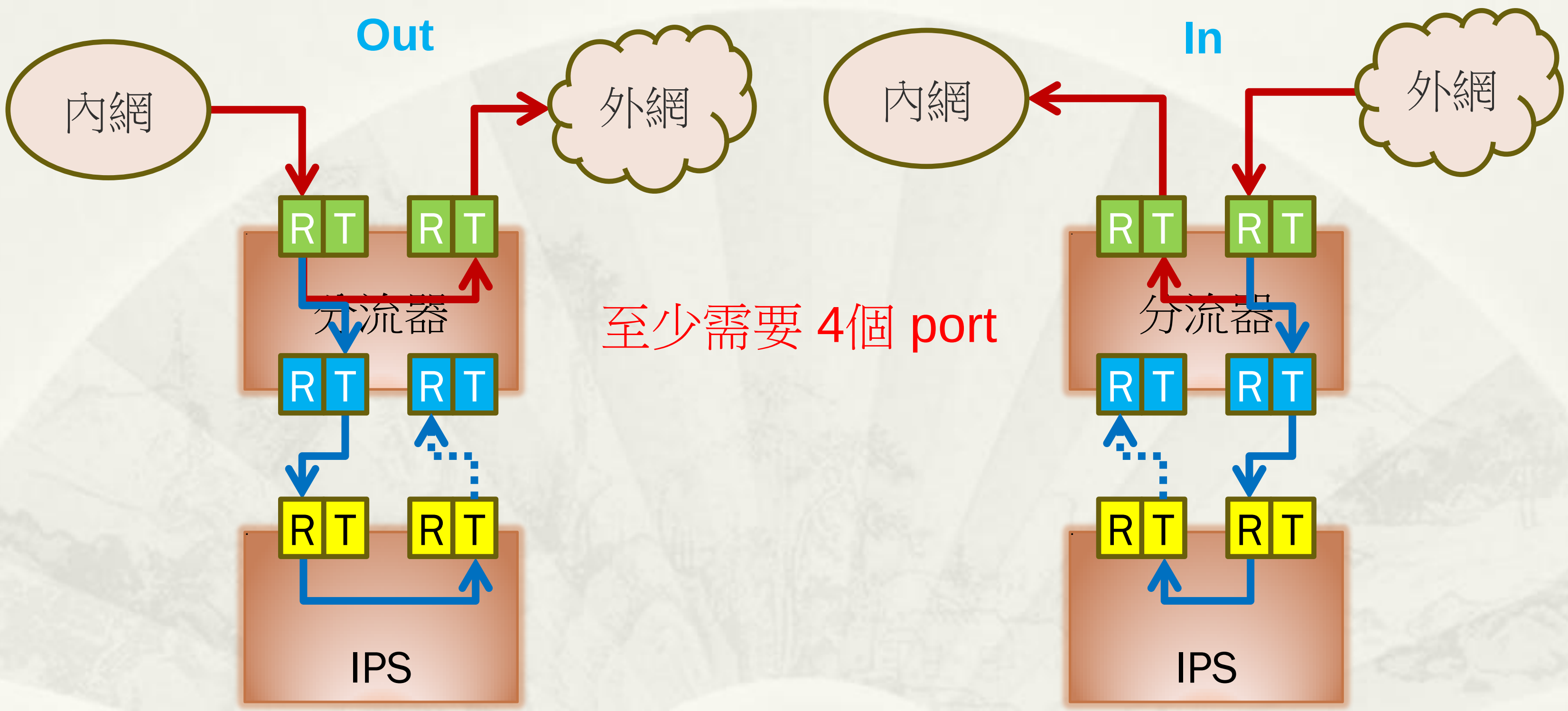
Bypass


Out
內網
R
T
R
T
外網
分流器
R
T
R
T
R
T
R
T
IPS
In
內網
外網
R
T
R
T
分流器
R
T
R
T
R
T
R
T
IPS
Inline Network
Inline Tool

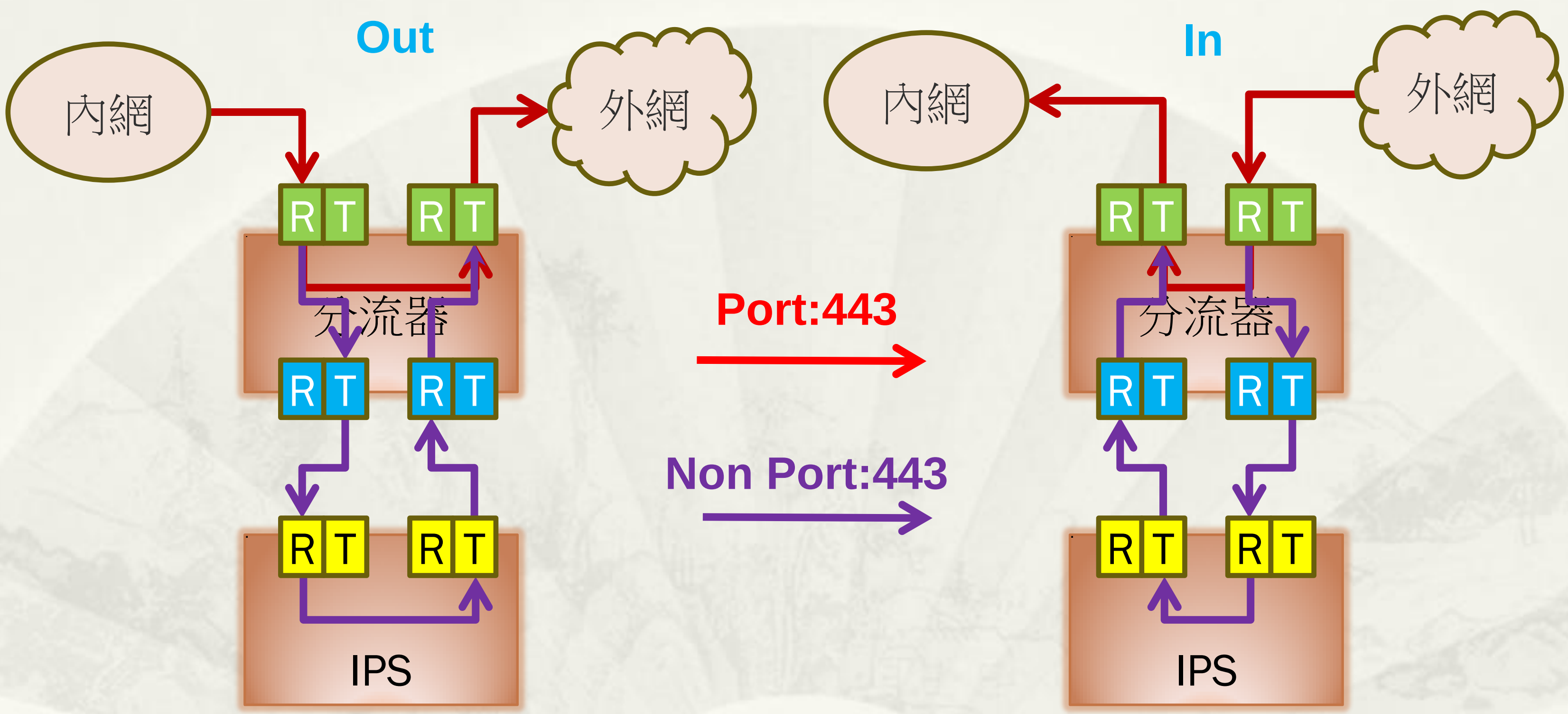
Inline


Out
內網
外網
R T
R T
分流器
R T
R T
R T
R T
IPS
至少需要 4個 port
In
內網
外網
R T
R T
分流器
R T
R T
R T
R T
IPS
Inline Network
Inline Tool

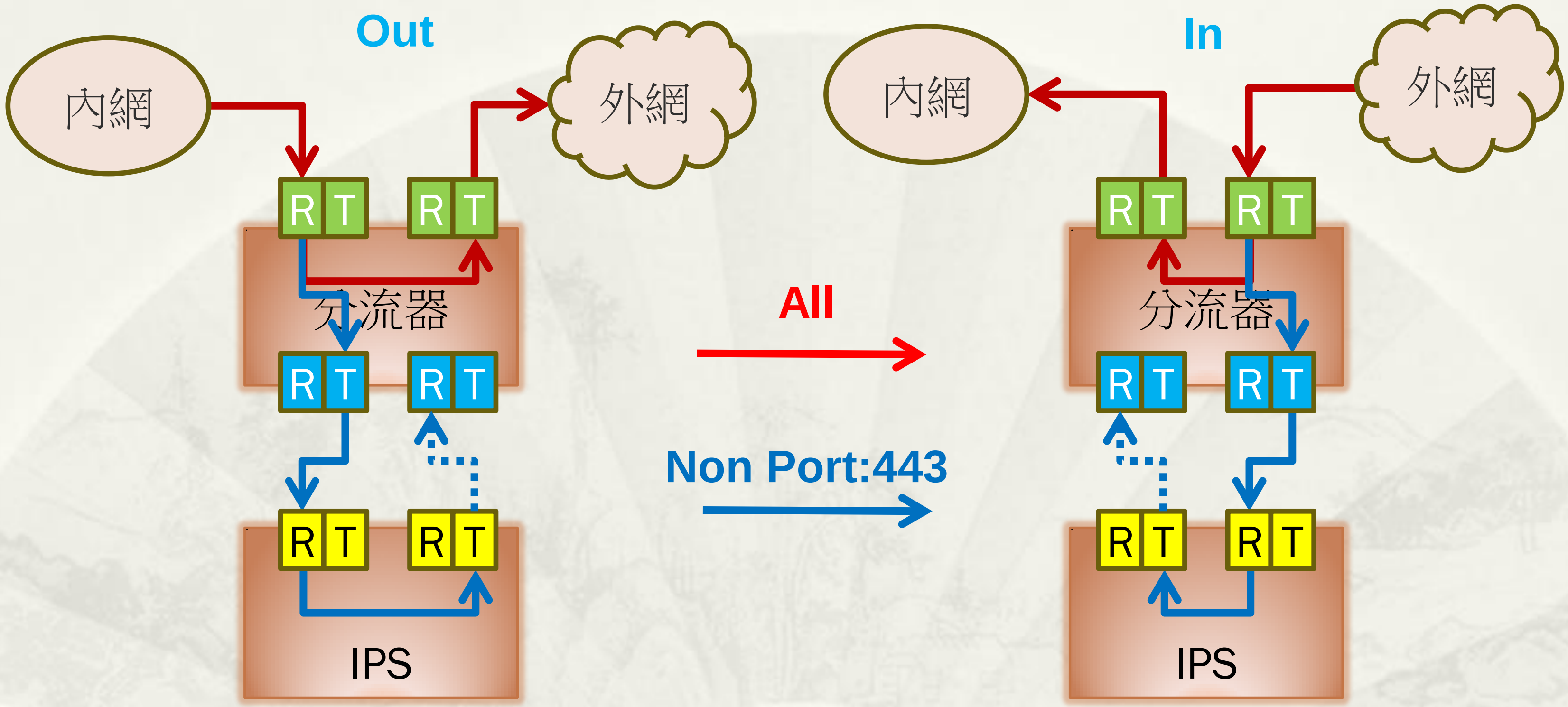
TAP


Out
內網
外網
R T
R T
分流器
R T
R T
R T
R T
IPS
至少需要 4個 port
In
內網
外網
R T
R T
分流器
R T
R T
R T
R T
IPS

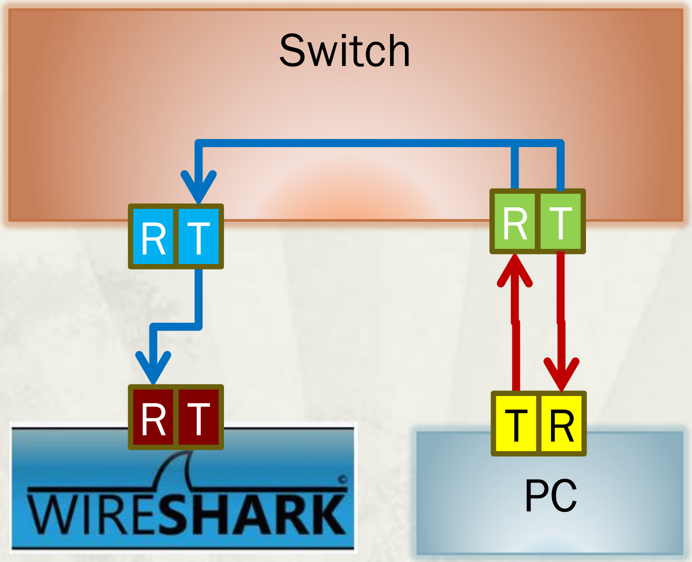
Selective Inline



Selective TAP

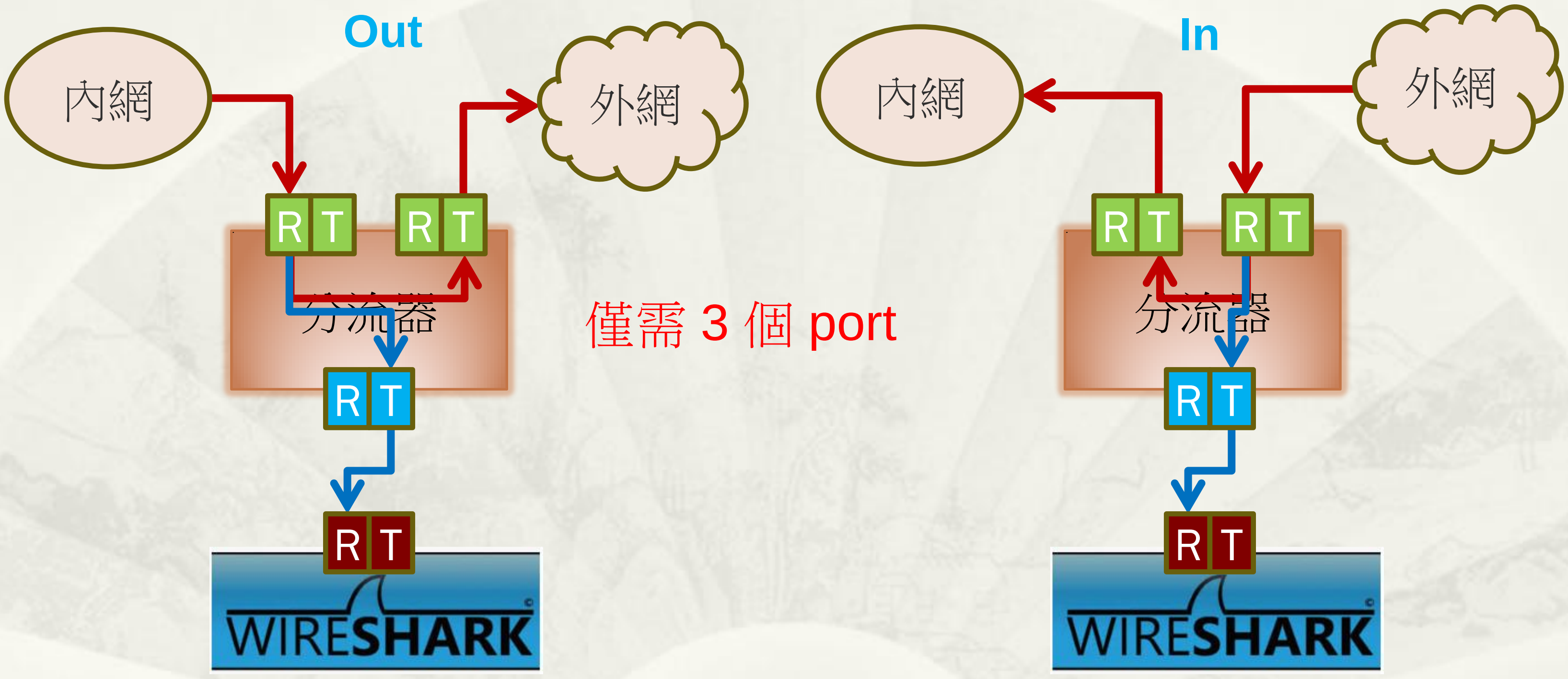


SPAN(Switched Port Analyzer) Mirror



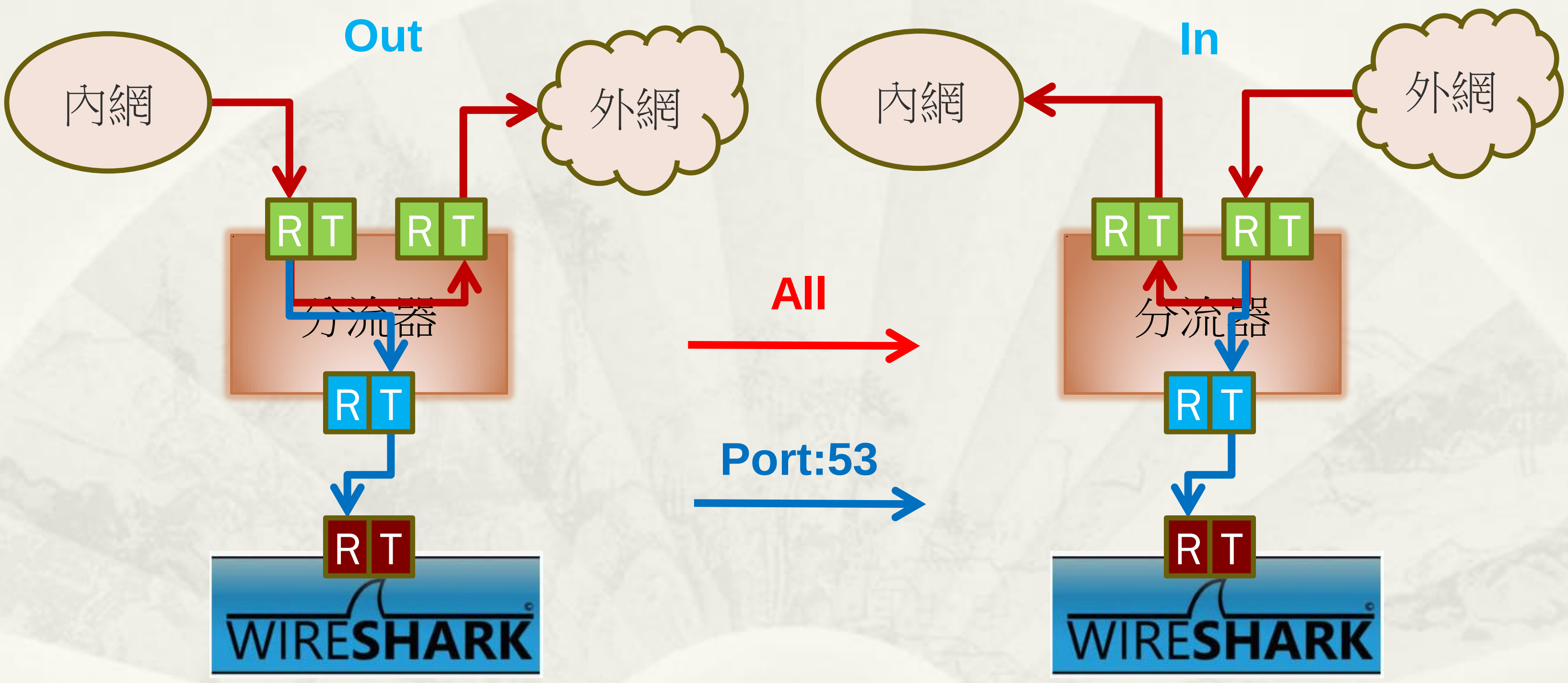
- Use Only 1 Port: RX + TX Mixed to TX
- Only One Direction Max Bandwidth
  - Full-duplex: 100/100 Mbps
  - One Direction: 100 Mbps

SPAN/Mirror
分流器

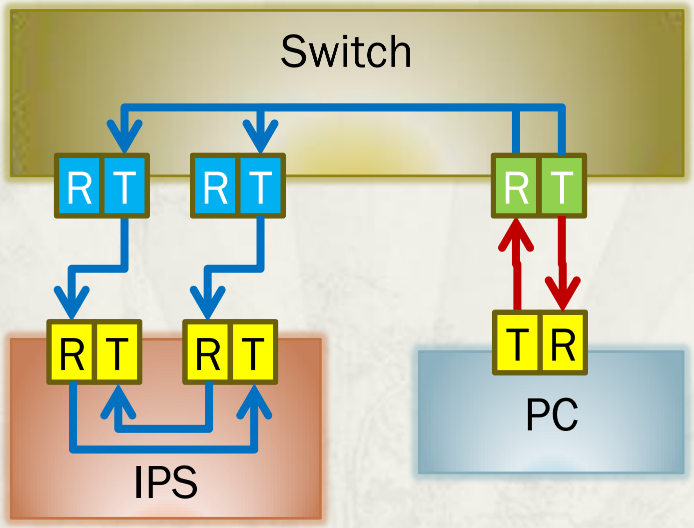


僅需 3 個 port

Selective SPAN/Mirror



SPAN/Mirror
模擬 TAP



有些 Switch 支援
Selective SPAN/Mirror

SPAN/Mirror

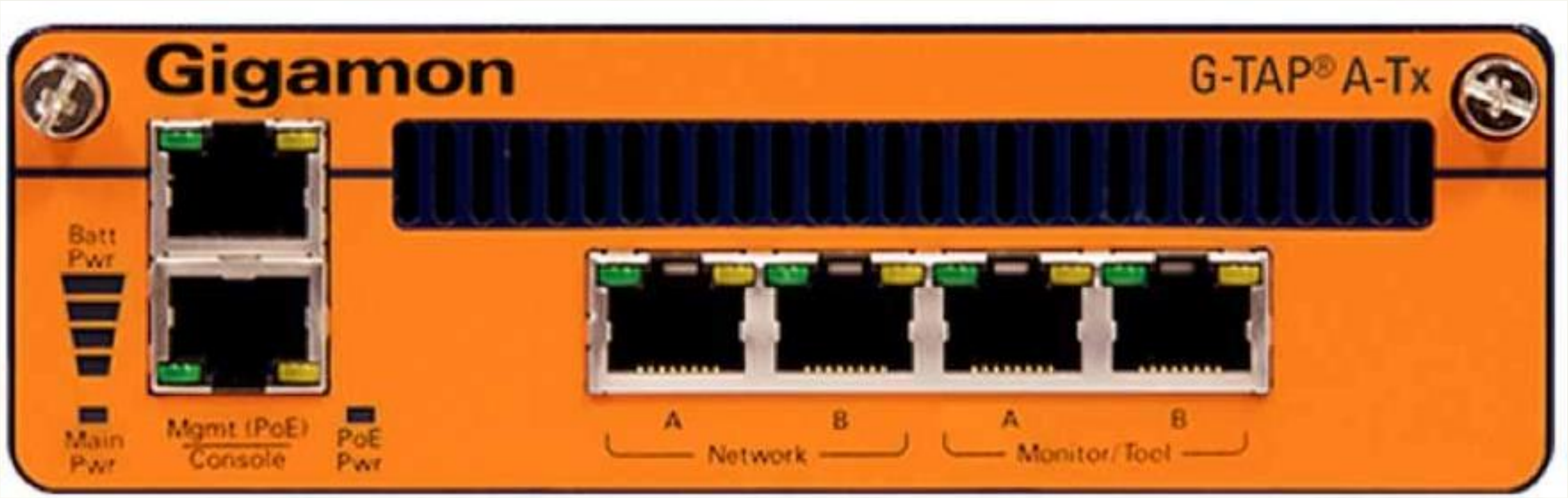
- 無法分辨封包 TX/RX 方向
- 解決方法
  - 使用 IP 網段: 內網可能有假造封包IP 而不準確
  - 使用 Src Mac/Dst Mac
  - Download/Upload 加上 Vlan tag
  - 使用 TTL
    - TTL= 64,128,254,255 -> 內網 IP

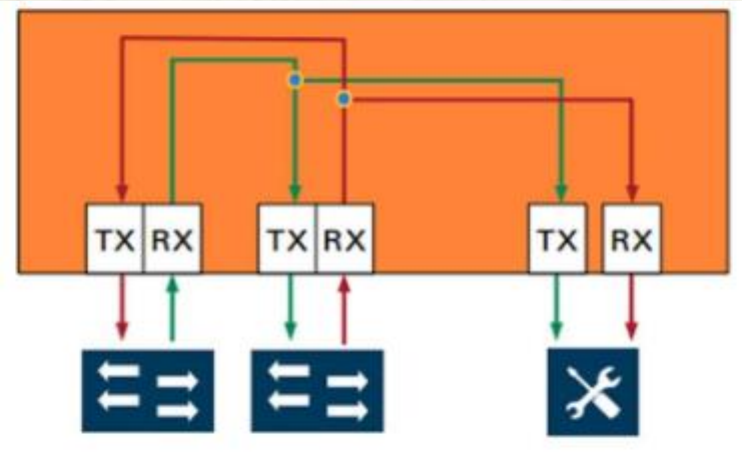
TAP
Splitter (1:3) 1分3/ 1進3出

TAP
Splitter (1:3)

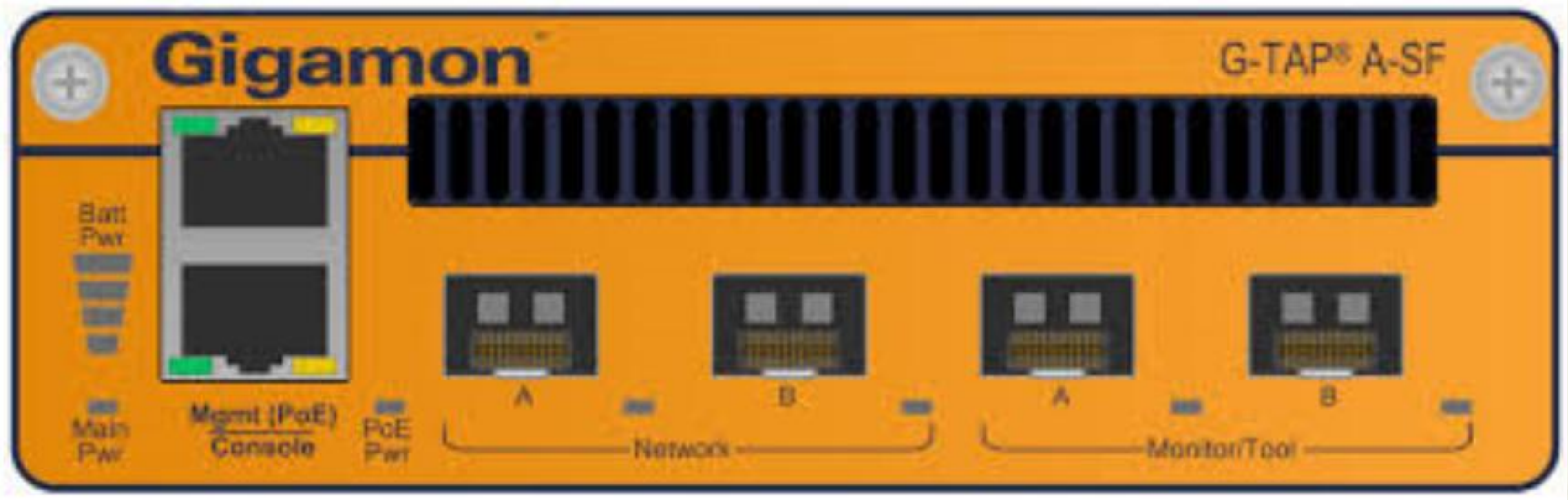
- To IPS 設備僅需接一條線

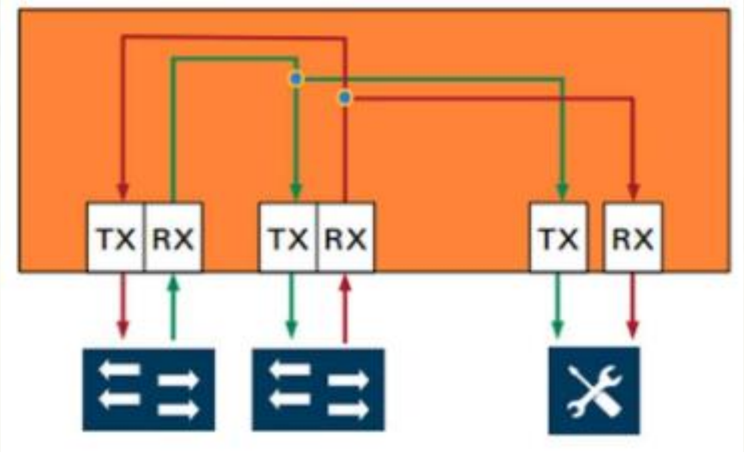
Gigamon TAP UTP





Gigamon TAP Fiber

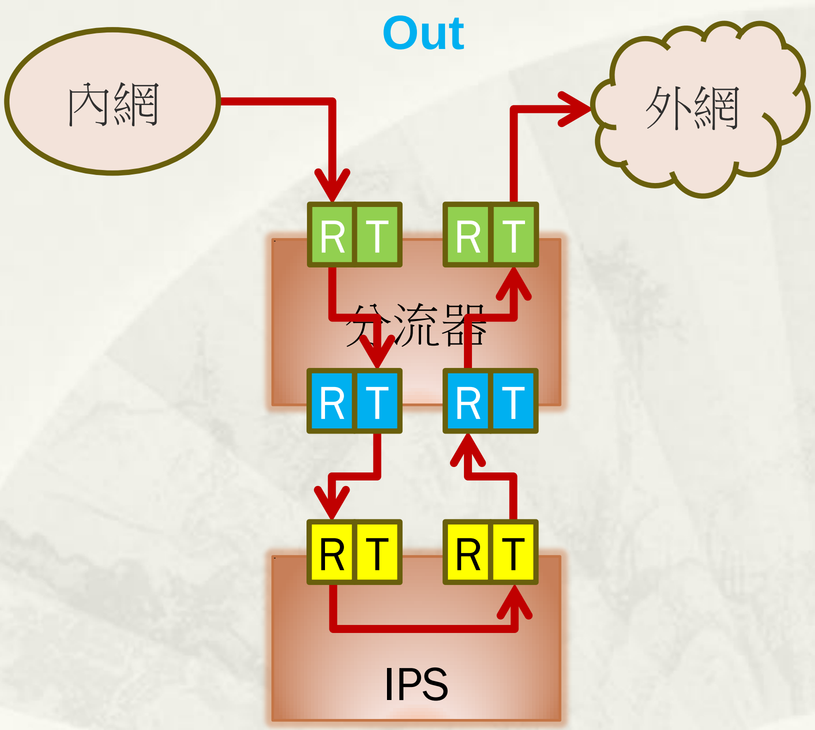




頻寬分流管理器評估

評估項目	功能說明	Spec
Selective Inline/Tap	Support Layer	Layer1 ~ Layer4: MAC addr, IP, Port Layer7 Layer(Wireshark): http agent, dns query name Application Layer(DPI): Skype, Line, ...
Physical ByPass	斷電切換 ByPass	光/電介面 非 SFP 可插拔
Logical/Software ByPass (Heart beat)	偵測 IPS 設備異常切換 ByPass	單向/雙向 Only 收/送 模擬 Client/Server

Inline to Bypass



- Physical Bypass
  - 停電
- Logical/Software Bypass
  - Hear beat
  - To IPS 實體線路中斷
  - IPS 當機/處理速度過慢

Physical Bypass Module

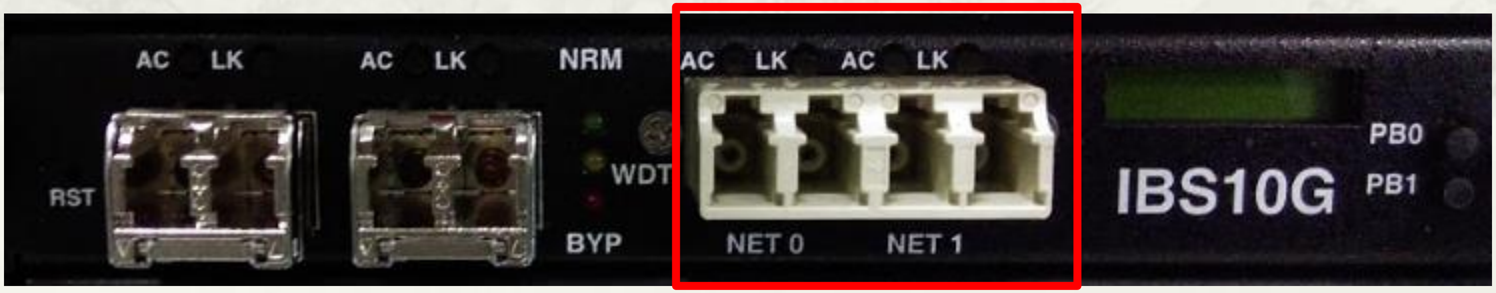
Gigamon HC1

上下一對

SourceFire IPS

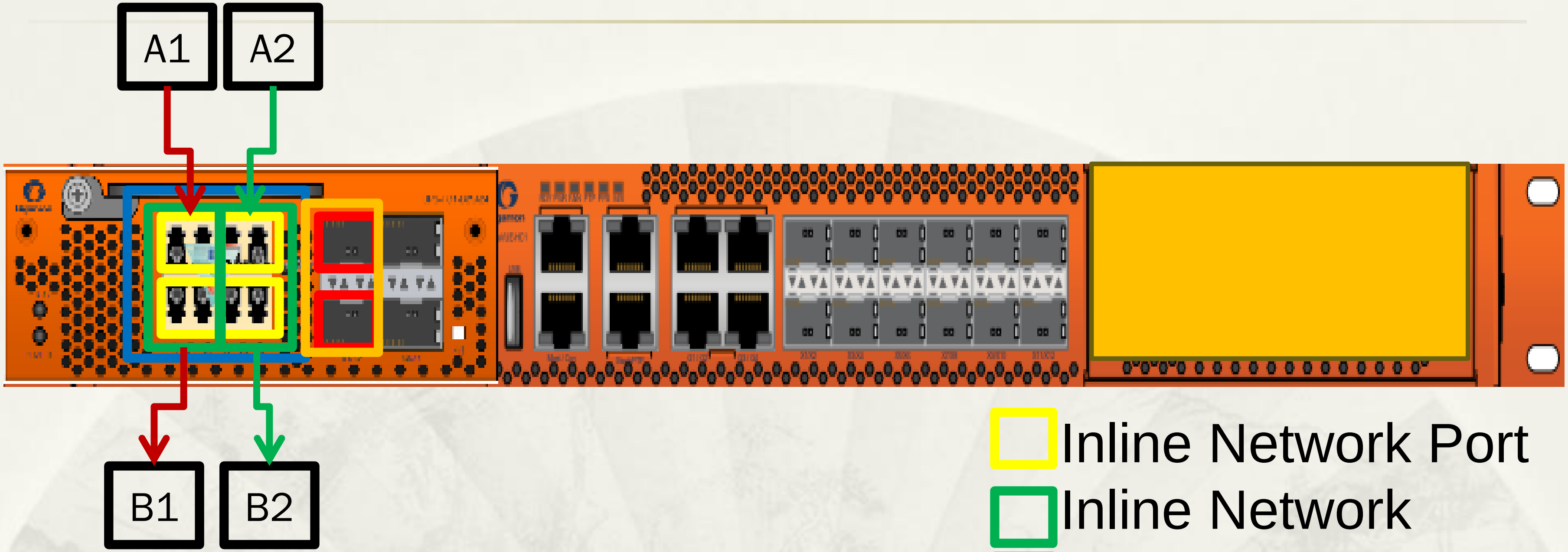
左右一對

Silicom Bypass Module



左右一對

Inline Network Group to Inline Tool

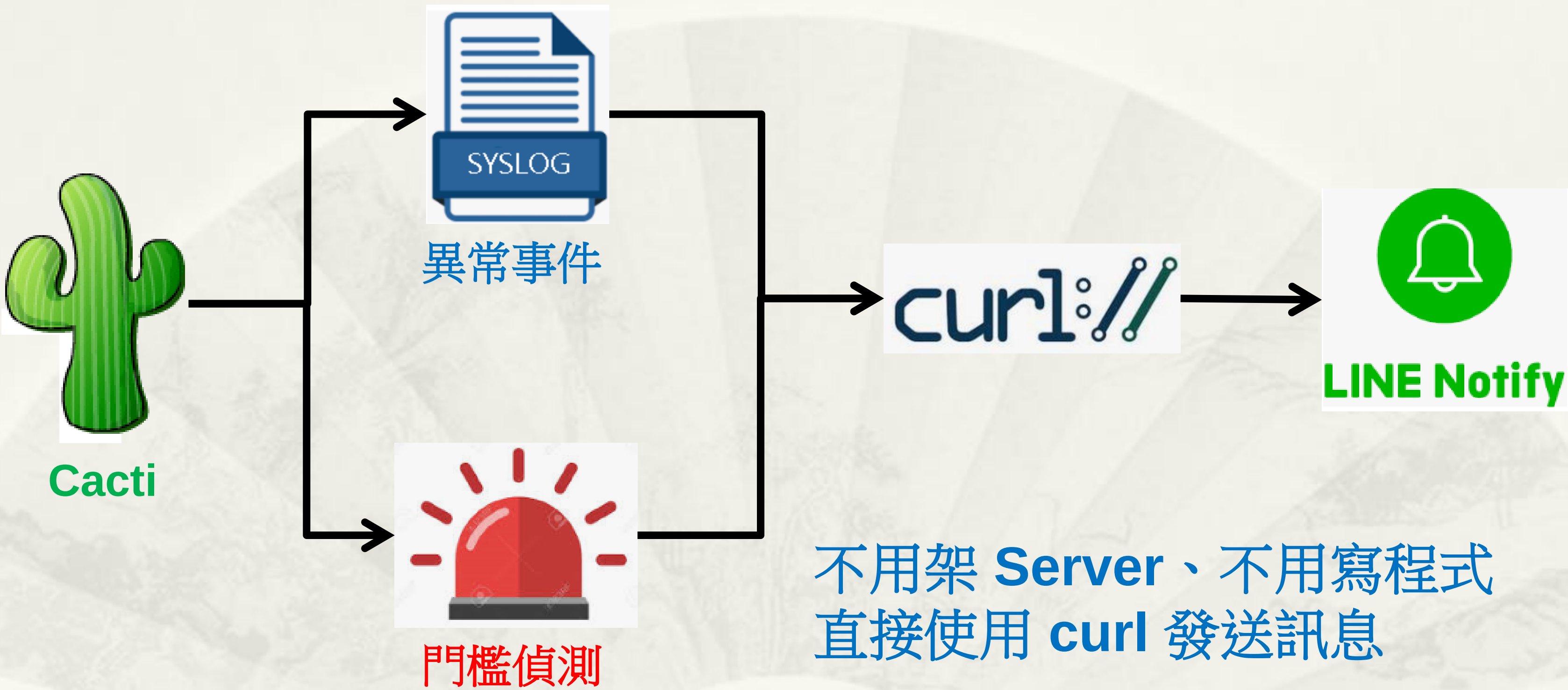


Inline Network Port
Inline Network
Inline Network Group

Inline Tool Port
Inline Tool

- 因為 A1 與 A2 流量會同時送到 Inline Tool
- 為了確保
  - 原 A1 流量 需從 B1 出去
  - 原 A2 流量 需從 B2 出去
- 在 Inline Tool 中流量會加上 Vlan id，出去後再拿掉

Cacti 結合 Line Notify



不用架 **Server**、不用寫程式
直接使用 **curl** 發送訊息

107年評審委員建議:
5.區網流量大幅成長，對於網管及資安服務應有配套規劃。

Cacti SYSLOG 異常事件

- 監控 ASR Router Log 異常事件

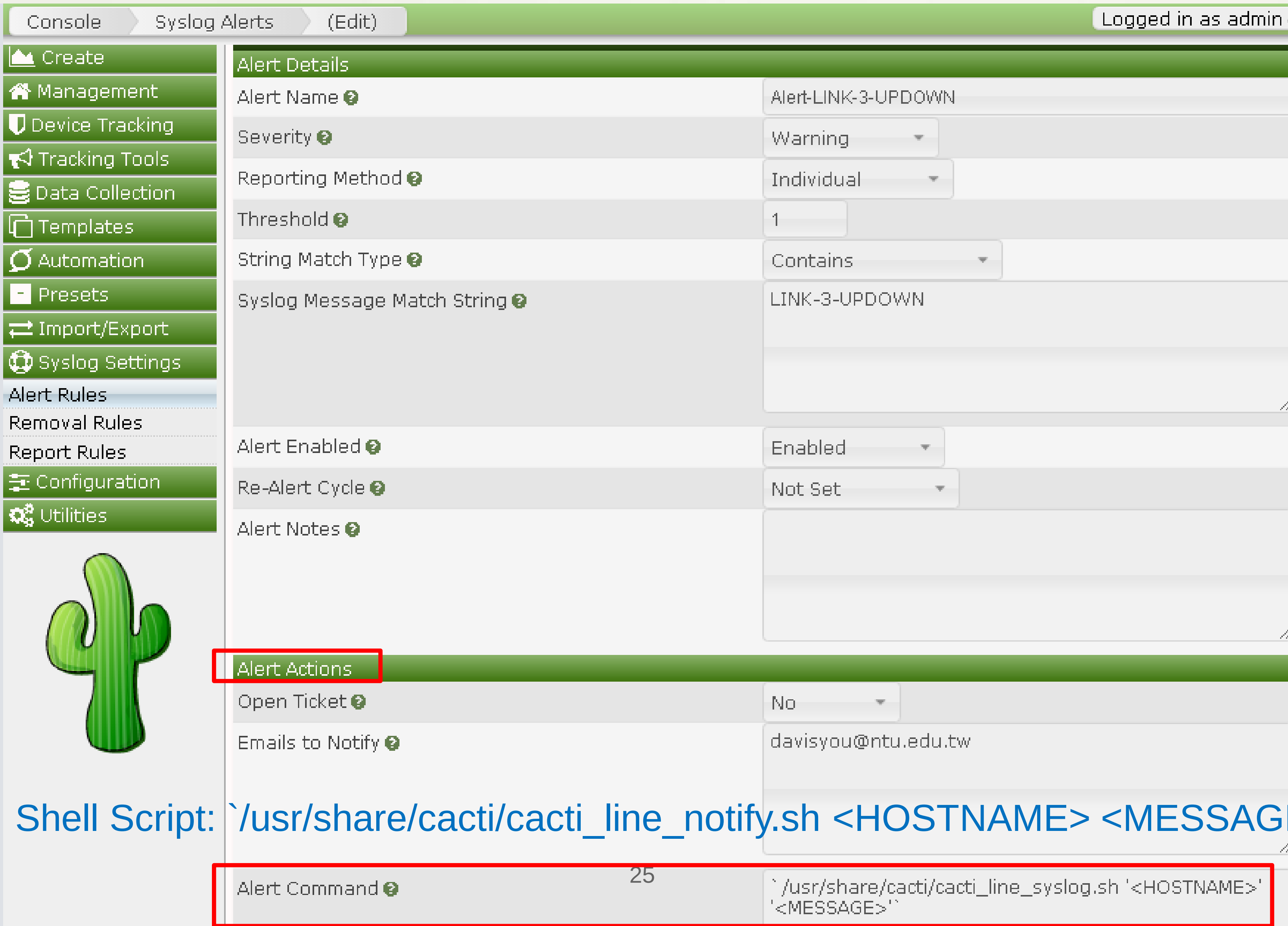
Alert Name**	Severity	Method	Threshold Count	Enabled	Match Type	Search String
Alert-AUTHEN_SUCCESS	Warning	Individual	N/A	Yes	Contains	AUTHEN_SUCCESS
Alert-LINEPROTO-5-UPDOWN	Warning	Individual	N/A	Yes	Contains	LINEPROTO-5-UPDOWN
Alert-LINK-3-UPDOWN	Warning	Individual	N/A	Yes	Contains	LINK-3-UPDOWN
Alert-LOGIN_SUCCESS	Warning	Individual	N/A	Yes	Contains	LOGIN_SUCCESS
logged command	Warning	Individual	N/A	Yes	Contains	logged command
OSPF-5-ADJCHG	Warning	Individual	N/A	Yes	Contains	OSPF-5-ADJCHG
OSPFv3-5-ADJCHG(ipv6)	Warning	Individual	N/A	Yes	Contains	OSPFv3-5-ADJCHG

事件: 有人成功登入 Router

LINE Notify

CCNET_Notify: 140.112.0.70RP/0/RP0/CPU0:Sep
6 15:49:07.861 : exec[65941]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'ntuadmin1' from '192.168.214.133' on 'vty1',

Cacti SYSLOG Alert Action

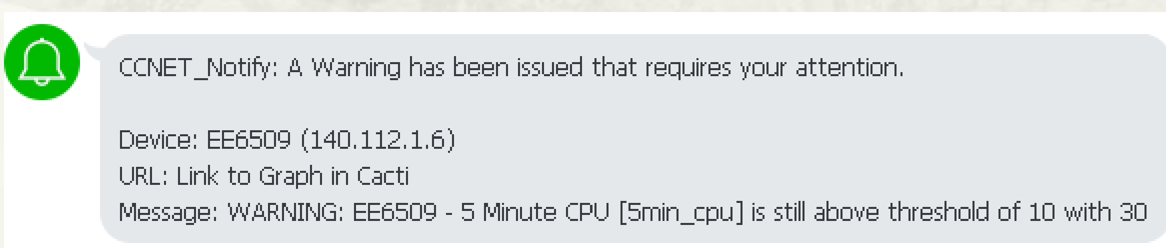


Shell Script: `/usr/share/cacti/cacti_line_notify.sh <HOSTNAME> <MESSAGE>`

Line Notify
Shell Script

- cacti_line_notify.sh
  - curl -v https://notify-api.line.me/api/notify \
  - -H 'Authorization: Bearer *Access_Token*' \
  - -F 'message="'$1'" \
  - -F 'message="'$2“

事件: CPU Usage 異常



Cacti 結合 Line Notify 優點

- 不需架設 Syslog Server
- 不需監控 Email Server 及 Parse 內容
- 不用寫程式(use curl only)
- 維護簡單且更即時

LINE BOT 即時網頁內容搜尋

4.2 Line Bot 即時網頁內容搜尋

Ptt 論壇: NTU 版

關鍵字:
Mail, 宿舍, 網路, 遭駭 …

BGPSTREAM

BGP Hijack

BGP Overage
BGP Hijacking
BGP Leaks
關鍵字:
ASN TW

LINE Notify

CVE®

Common Vulnerabilities
and Exposures

關鍵字
Cisco, Microsoft, Apache ….

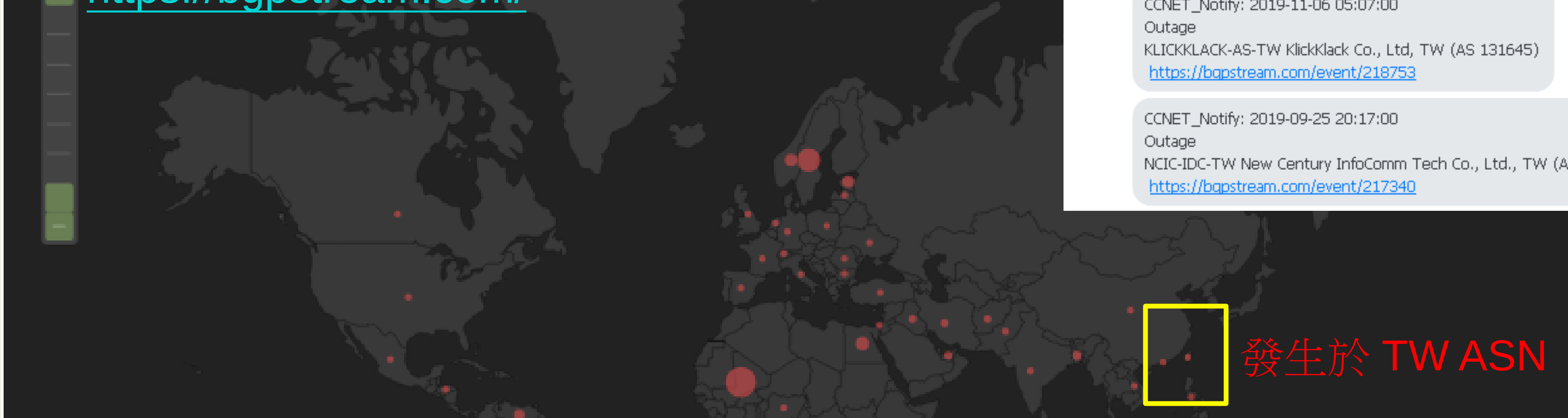
107年評審委員建議:
5.區網流量大幅成長，網管及資安服務應有配套規劃。

庶民訊息~快速掌握~
ptt.cc 鄉民的正義

BGPSTREAM

BGP Hijack 即時訊息

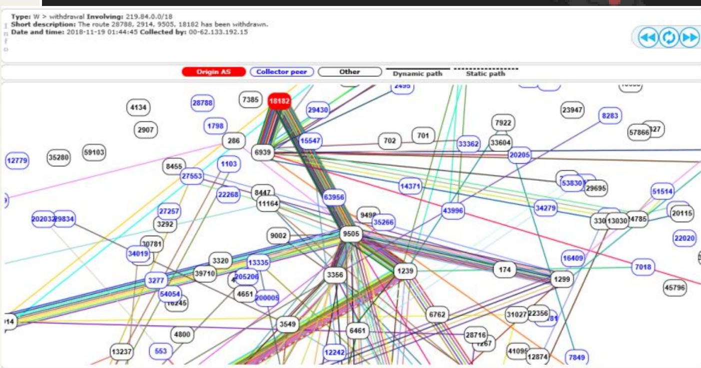
https://bgpstream.com/



CCNET_Notify: 2019-11-11 20:50:00
Outage
KLICKKLACK-AS-TW KlickKlack Co., Ltd, TW (AS 131645)
https://bgpstream.com/event/219156

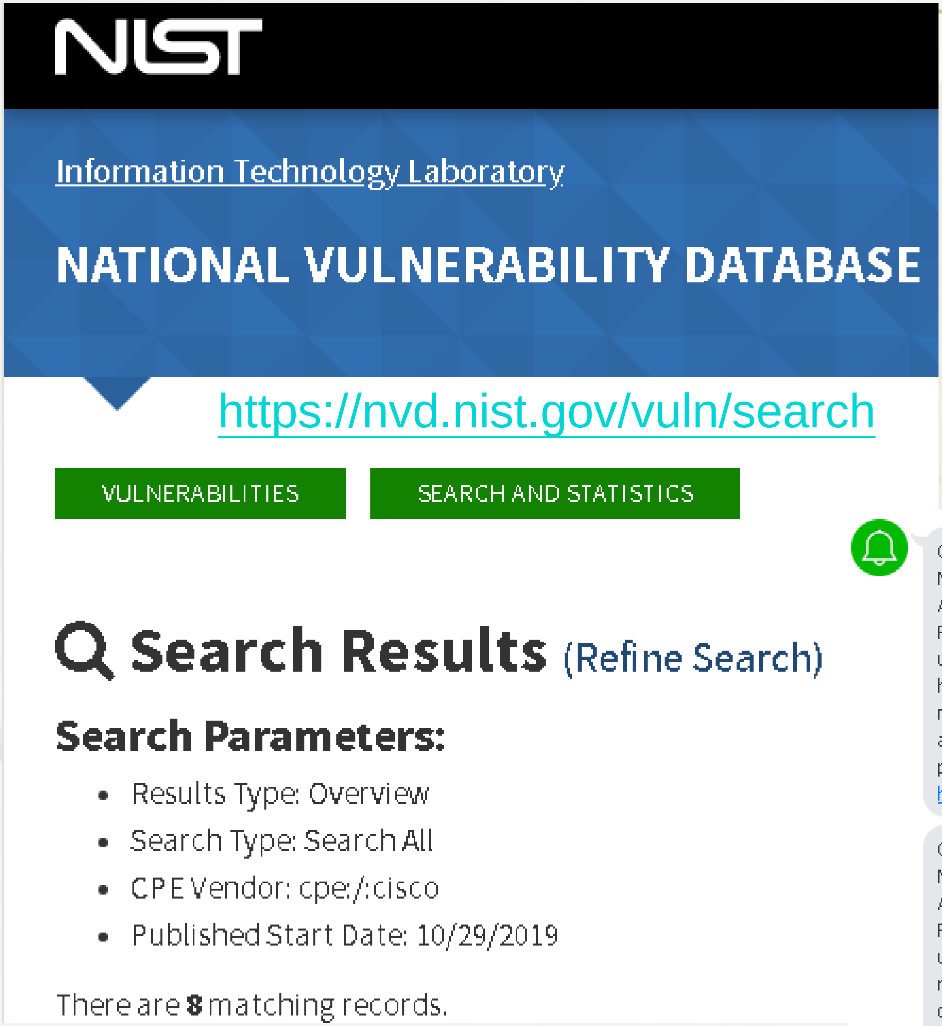
CCNET_Notify: 2019-11-06 05:07:00
Outage
KLICKKLACK-AS-TW KlickKlack Co., Ltd, TW (AS 131645)
https://bgpstream.com/event/218753

CCNET_Notify: 2019-09-25 20:17:00
Outage
NCIC-IDC-TW New Century InfoComm Tech Co., Ltd., TW (AS 131586)
https://bgpstream.com/event/217340



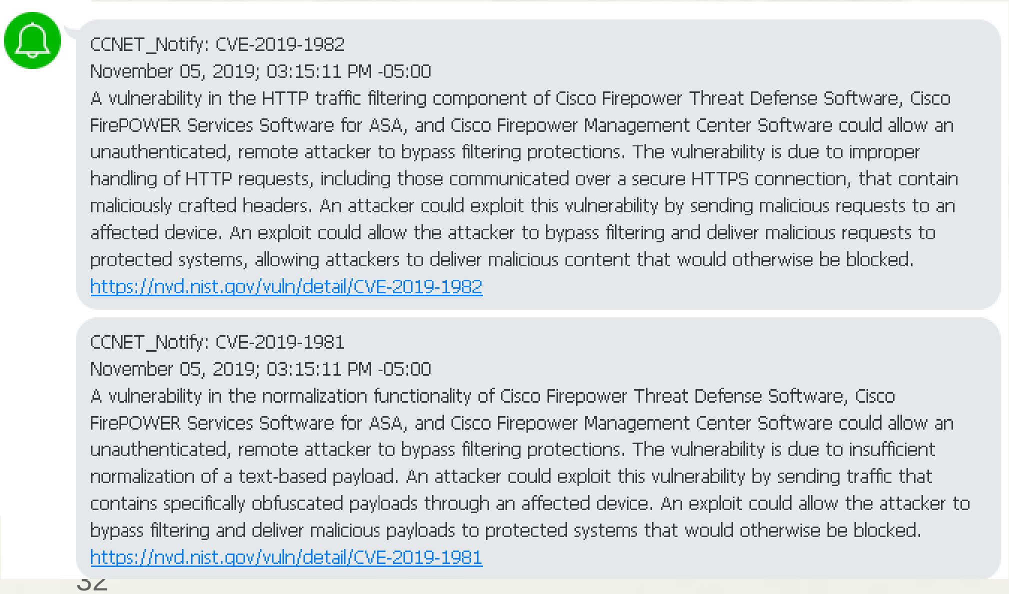
Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Outage		NETCONNECTWIFI-AS Net Connect Wifi Pvt Ltd, IN (AS 133973)	2019-05-06 06:44:00	2019-05-06 06:48:00	More detail
Possible Hijack		*Expected Origin AS:* JAHIZ, LB (AS 209265) *Detected Origin AS:* Beirut-Lebanon, LB (AS 9051)	2019-05-06 06:39:01		More detail
BGP Leak		*Origin AS:* SSALIANDCO-AS-AP S S Ali and Co, BD (AS 136027) *Leaker AS:* AAMRA-ATL-BD Aamra technologies limited, BD (AS 58601)	2019-05-06 06:35:22		More detail

資安漏洞~快速掌握~
CVE Database



https://nvd.nist.gov/vuln/search

產品範圍:
Cisco, Microsoft, Apache ….



To Do List

- 首頁網站內容是否被竄改
- 校內網段攻擊/被攻擊
- Talos 黑名單搜尋
- Zero day
- RSS 訂閱
- 個人~暗黑應用
  - ptt 演場會門票版
    - ‘急售’, ‘超低價‘, ’破盤’

區網群組

簡報完畢
謝謝