

從硬體攻擊手段來解開機殼下的美麗祕密：網路通訊設備安全分析

Ta-Lun Yen
Senior Vulnerability Researcher,
TXOne Research

重大聲明

- 此議程不包含任何 0-day。
- 此研究有其它重大發現，請密切專注我們後續發表。

特別銘謝

- 國家資通安全院 — 練喆明，韌性架構總顧問
- 數位發展部資通安全署
- TXOne – Sheng-Hao Ma、Canaan Kao 與其他所有人

吾輩所作種種之事

- 「此研究旨在確保此等設備是真正意義上的安全，並在真正的攻擊者出現前搶先發現可能被利用的安全漏洞。」



「如果我是敵國，會怎麼攻擊你的國家？」

網路攻防與戰爭

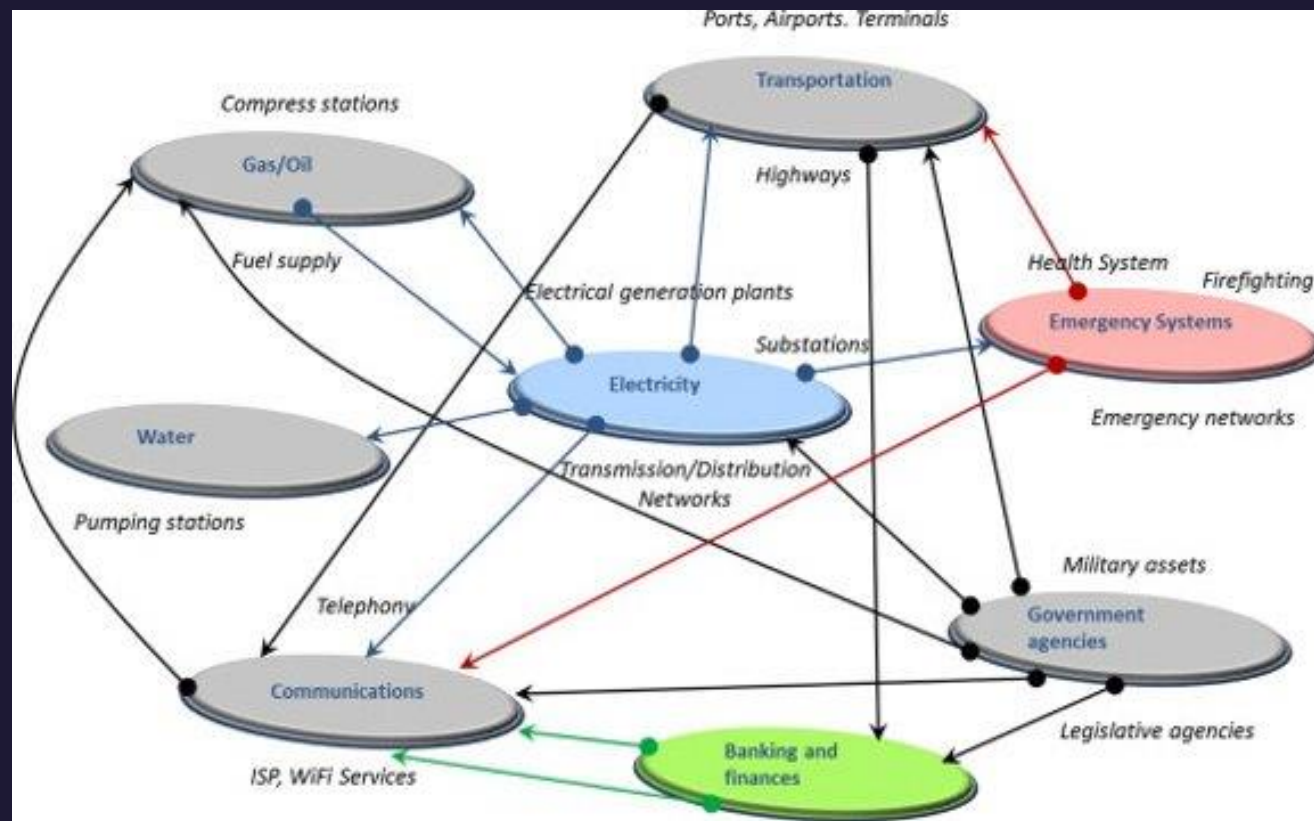
- Myth: 「網路攻防會是戰爭關鍵因素之一」
 - 「打敗敵人，摧毀其工業，佔領其土地是可能的，但如果其人民心中燃起抵抗的精神，誰都不能宣稱獲得勝利。」
——謝奕旭，復興崗學報，民 95，87 期，251-284
- 「戰爭僅是政治伴以另一個手段的延伸。」
—— Carl von Clausewitz
 - 戰爭的母體是政治；政治鬥爭的目的即是消滅敵人。
 - 戰爭是消滅敵人的手段之一。
- 「...網路攻擊會持續成為政治戰的手段之一。」
——CSIS, "Cyber Operations during the Russo-Ukrainian War"



當關鍵基礎設施成為一種武器

兩種武器化關鍵基礎設施的可能

- 影響真正影響人身安全的事物
 - 2008 俄羅斯-喬治亞戰爭——輸油管線爆炸
 - 假設情境：颱風汛期使水壩過度蓄水/非預期洩洪
- 影響國家運作順暢事物——通訊為萬物之母



Q: 如何打擊一個國家的電信網路？

- 「妨礙」（網路不通）
 - 物理破壞/物理攻擊電信骨幹？
 - 可能難—我們不是 Snake、不想被槍射
 - 可能簡單—喬治亞阿罵 + 鋸子
- 「佔領」（設備佔領）
 - 控制該國內夠多的網路設備？
 - 可能難，但相對容易、持久
 - 數量夠多，即成為王
 - 什麼東西是：到處都有、不能輕易替換、而且連線到骨幹上的？



網路設備挑選

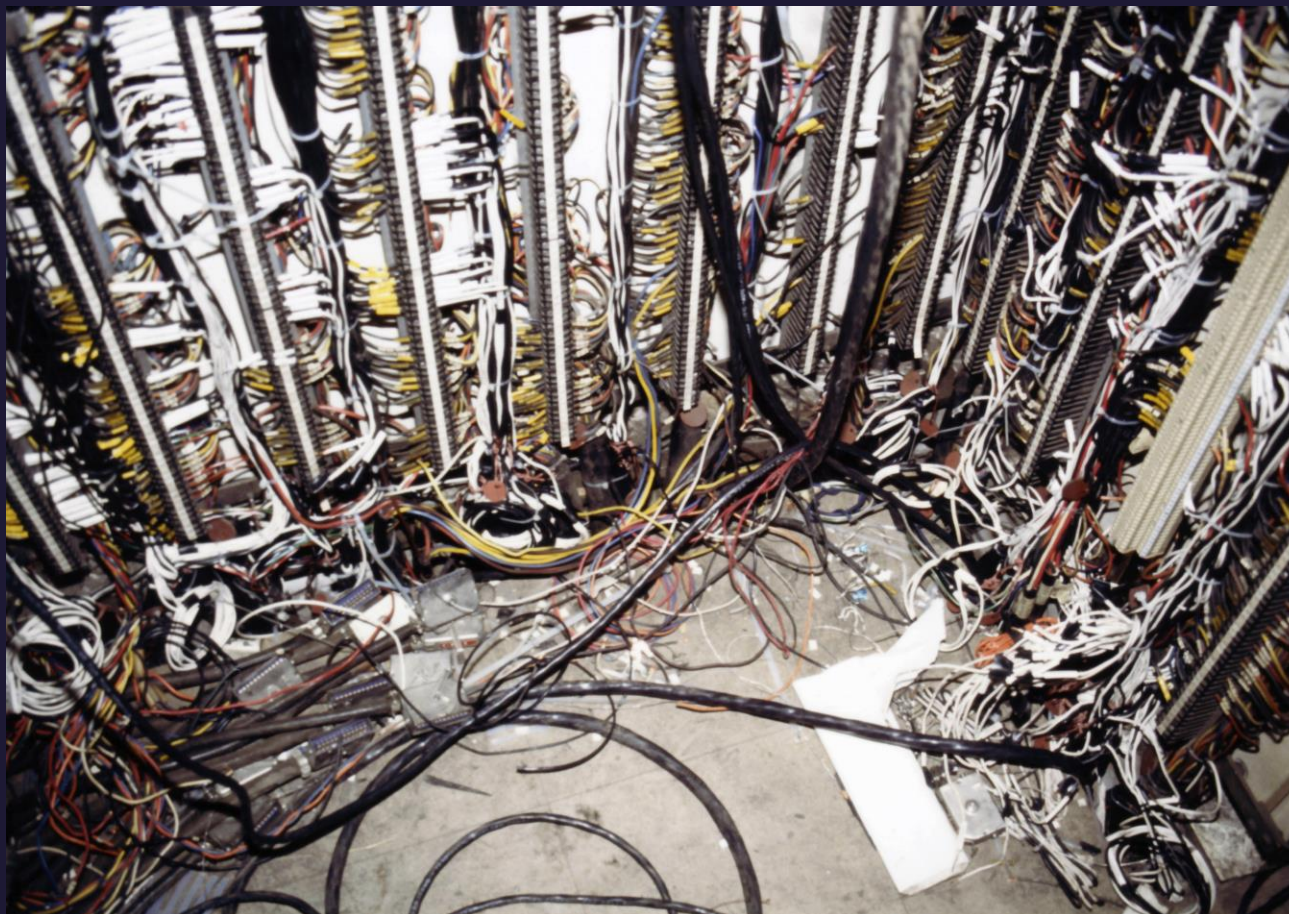
- 攻擊某夠多使用量的網路設備？
 - 可能會出現在敵國製網路設備或受供應鍊影響的產品中
 - 優勢：防守方初期管控困難
 - 問題：型號破碎化、產品可被禁售、產品可透過媒體被快速污名化等
- 攻擊公發終端網路產品
 - 型號統一化、無法被禁售、難以被防守或快速更換

名詞解釋 / FTTH ONT/ONU/CPE 們

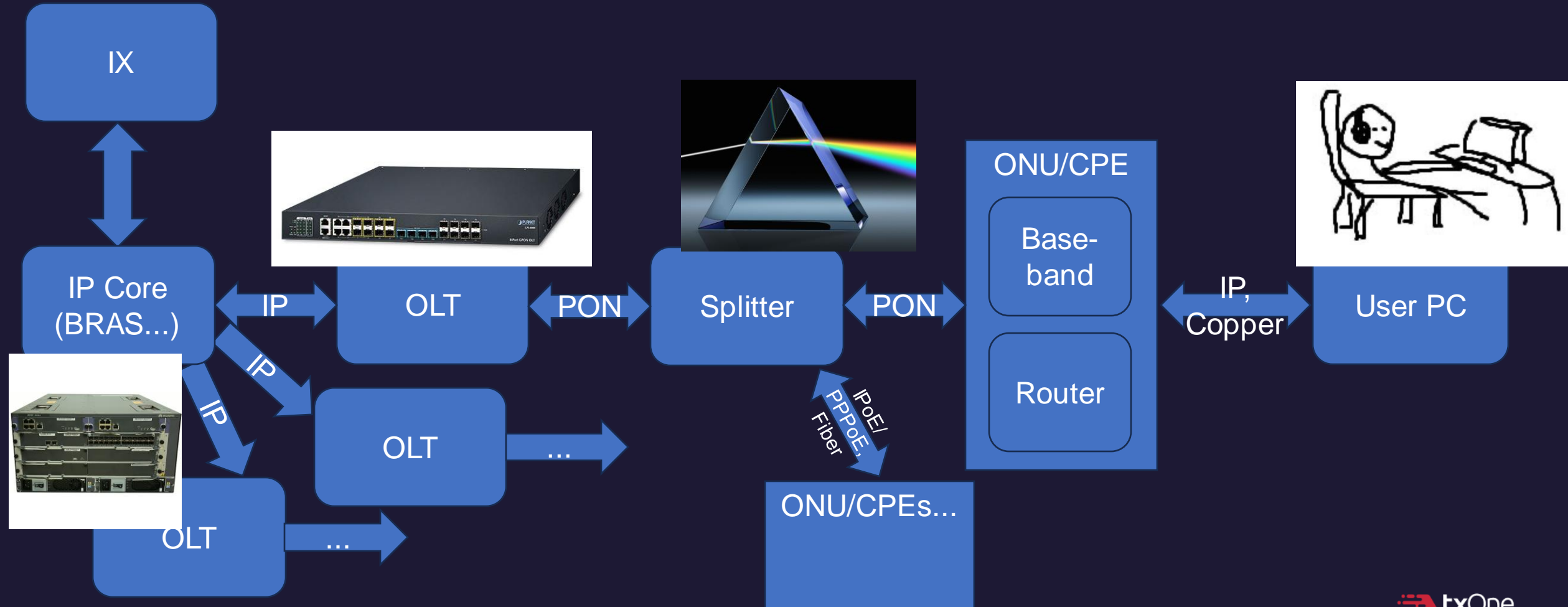
- OLT (Line Terminal) : ISP 端光纖交換器
- ONT (Termination) : 用戶端光<->電
- ONU (Unit) : 用戶端一體機



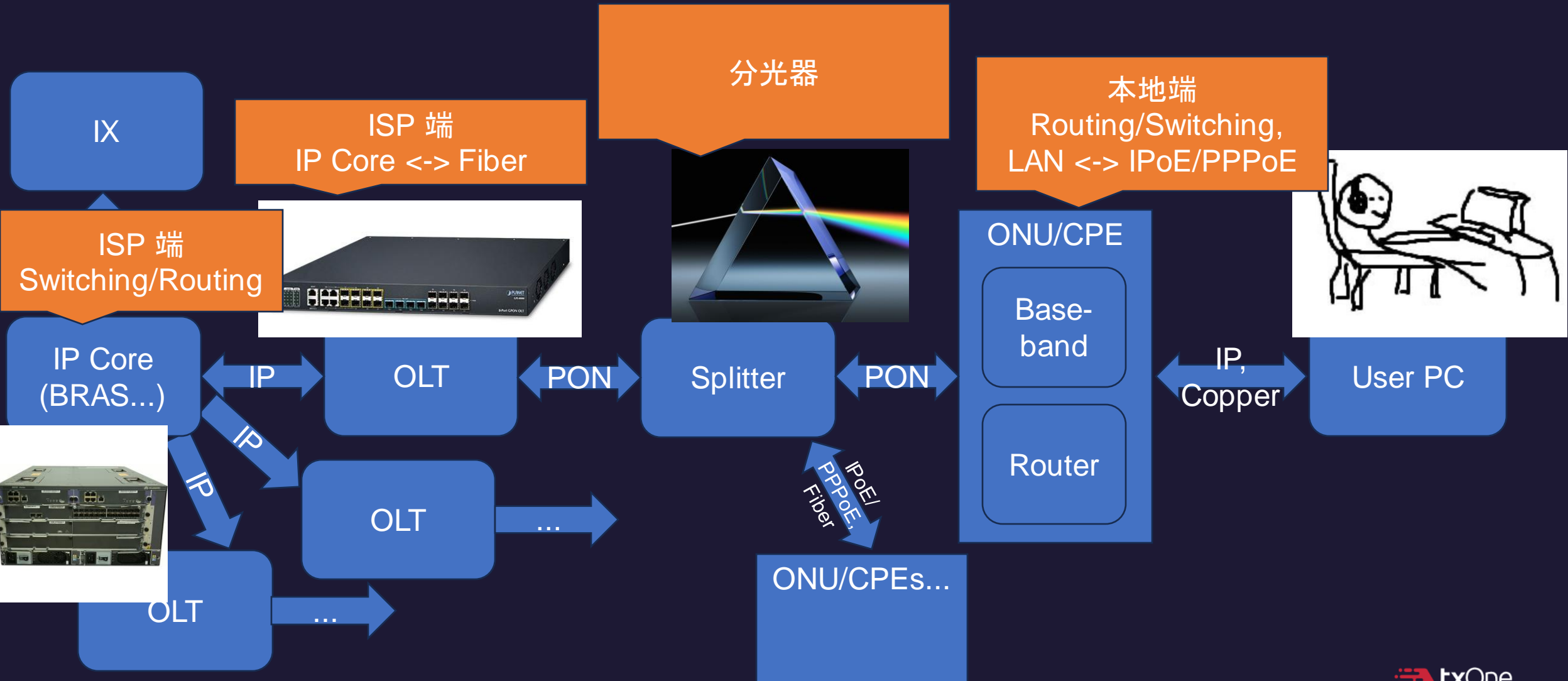
你以為的 FTTH 架構



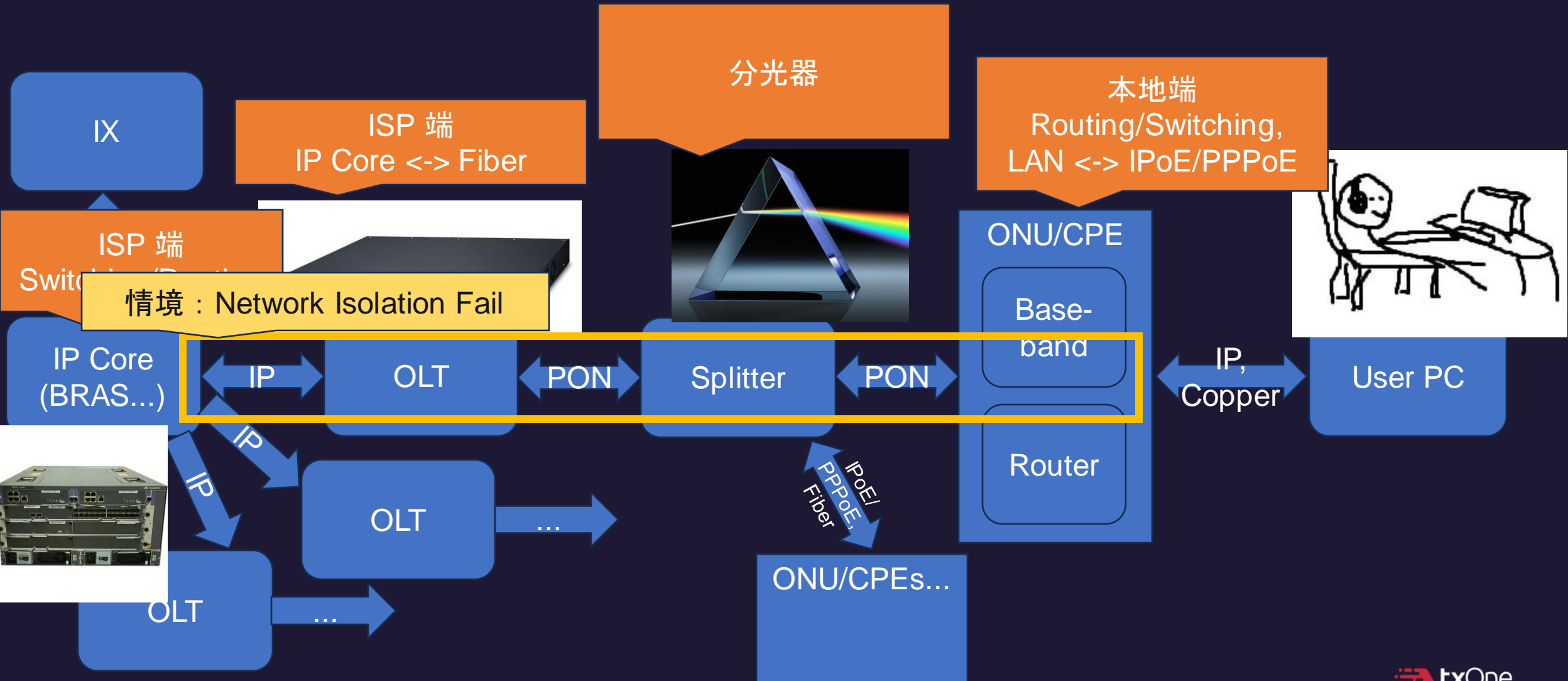
通訊架構角度 — GPON FTTH 架構



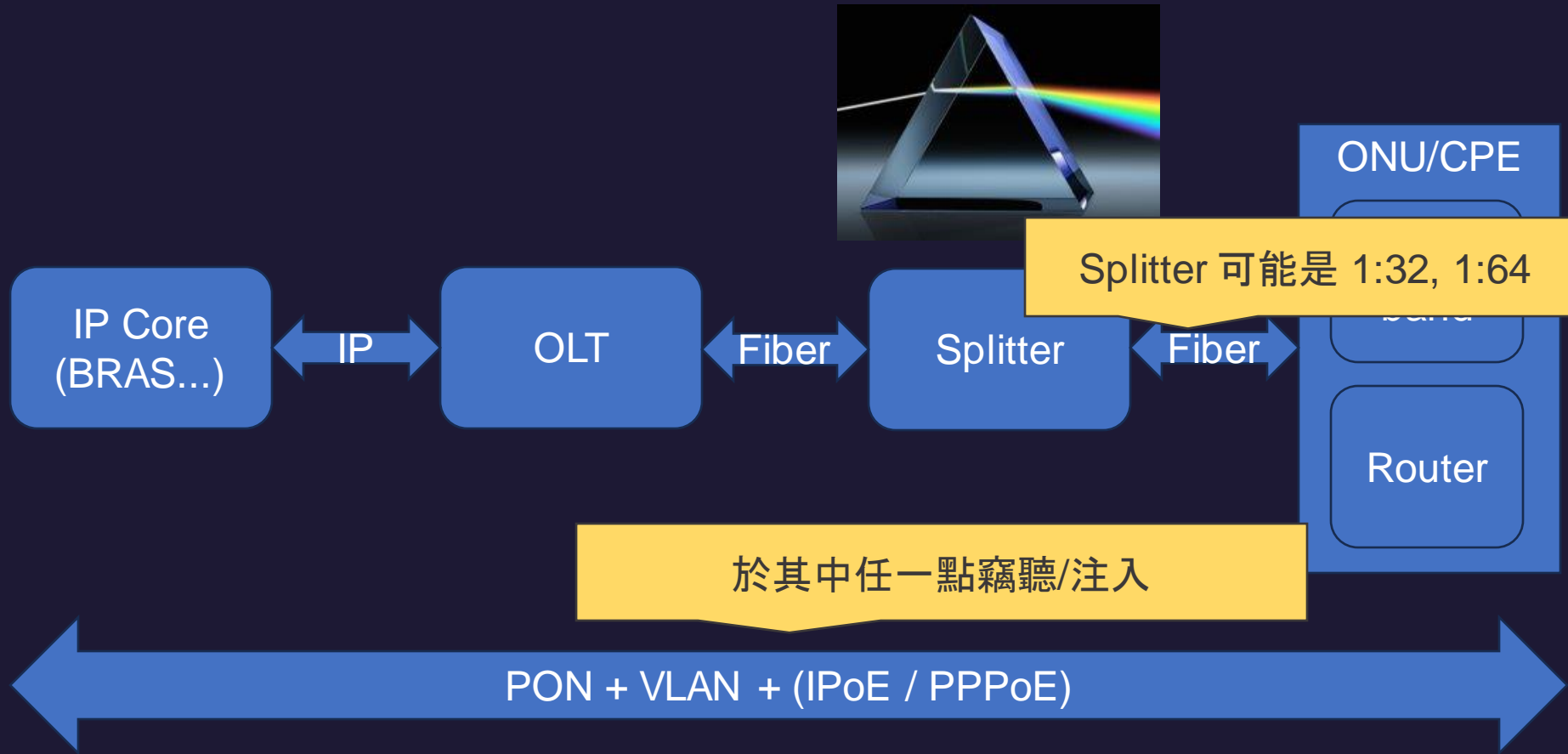
通訊架構角度 — GPON FTTH 架構



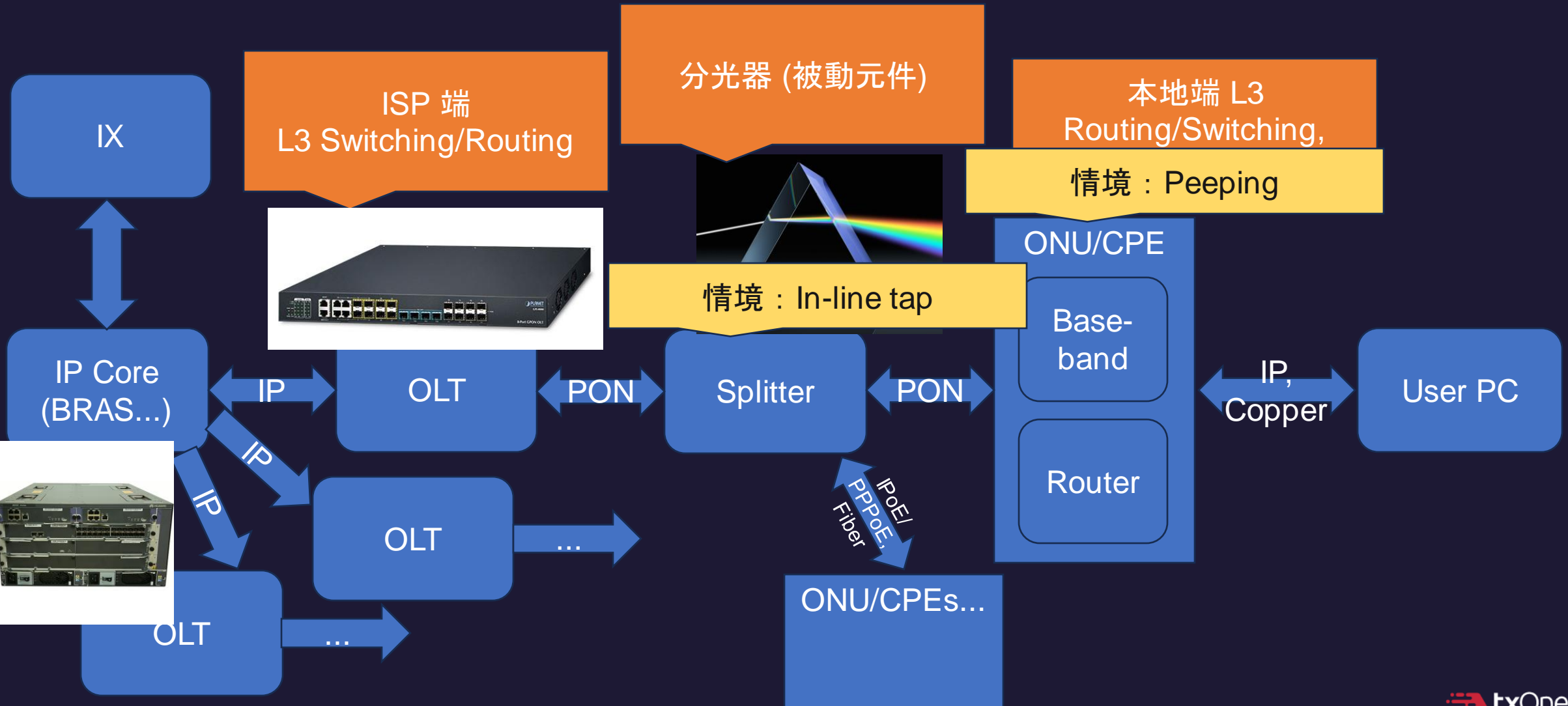
通訊架構角度 — GPON FTTH 架構



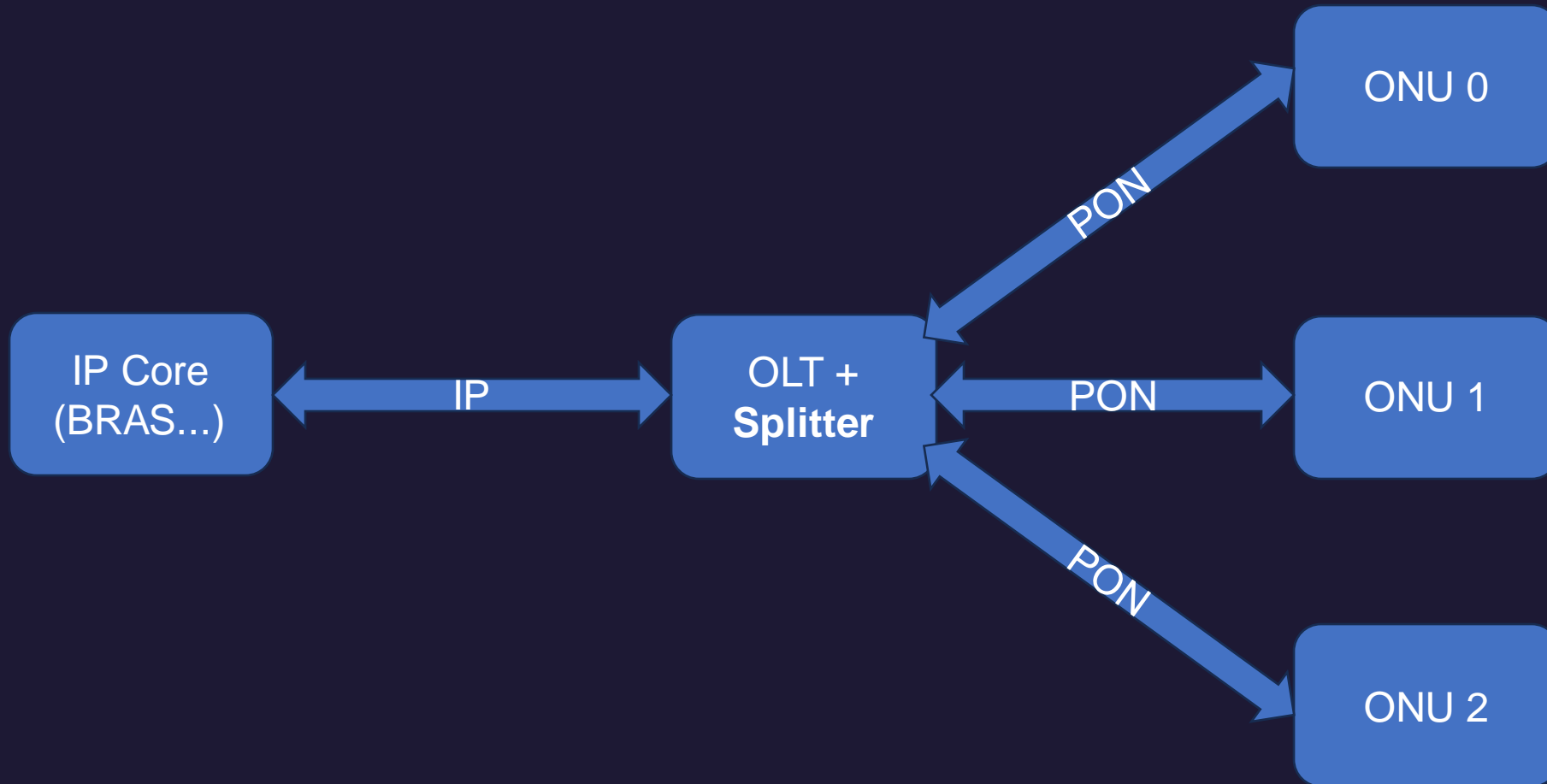
IPoE/PPPoE Isolation



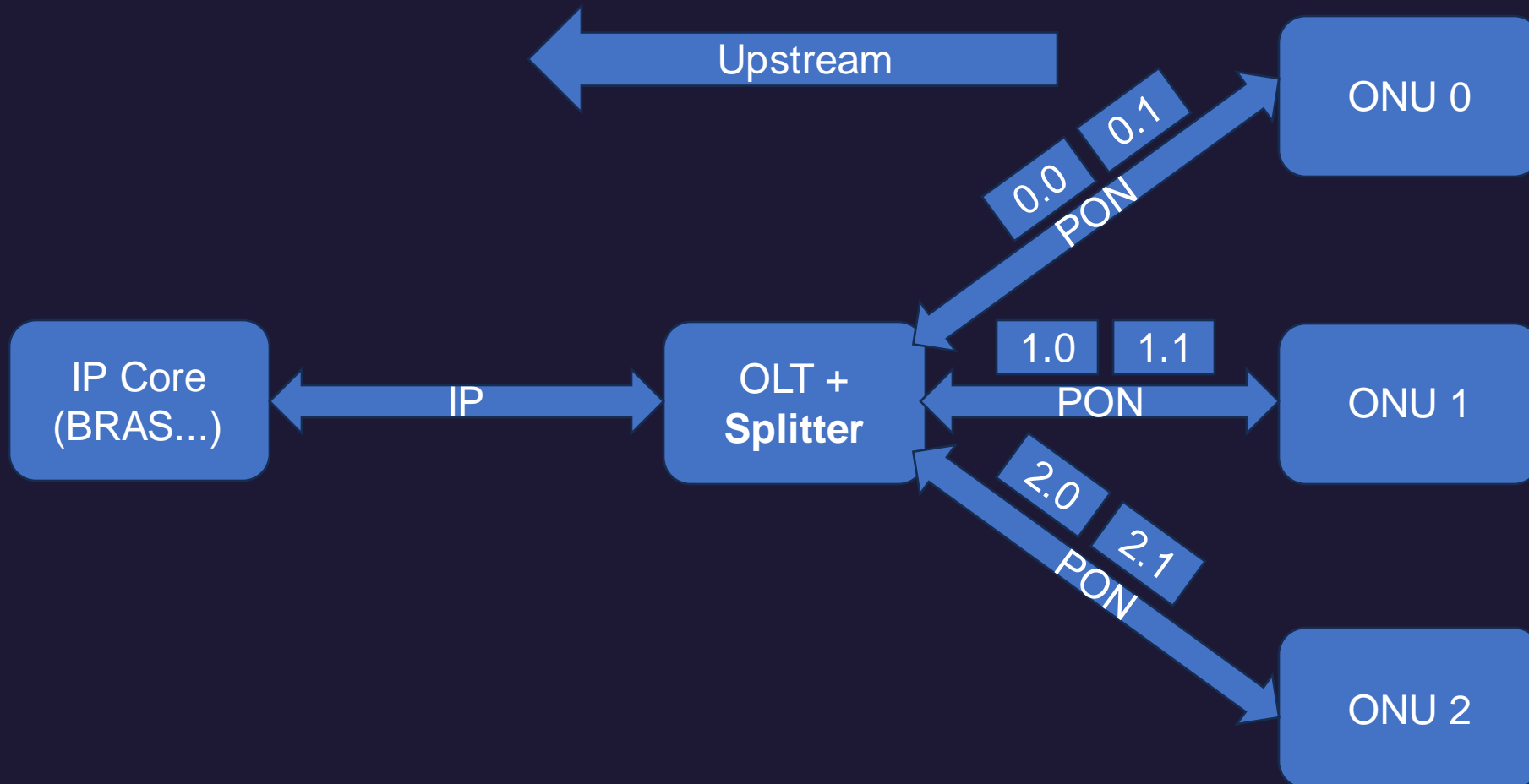
通訊架構角度 — GPON FTTH 架構



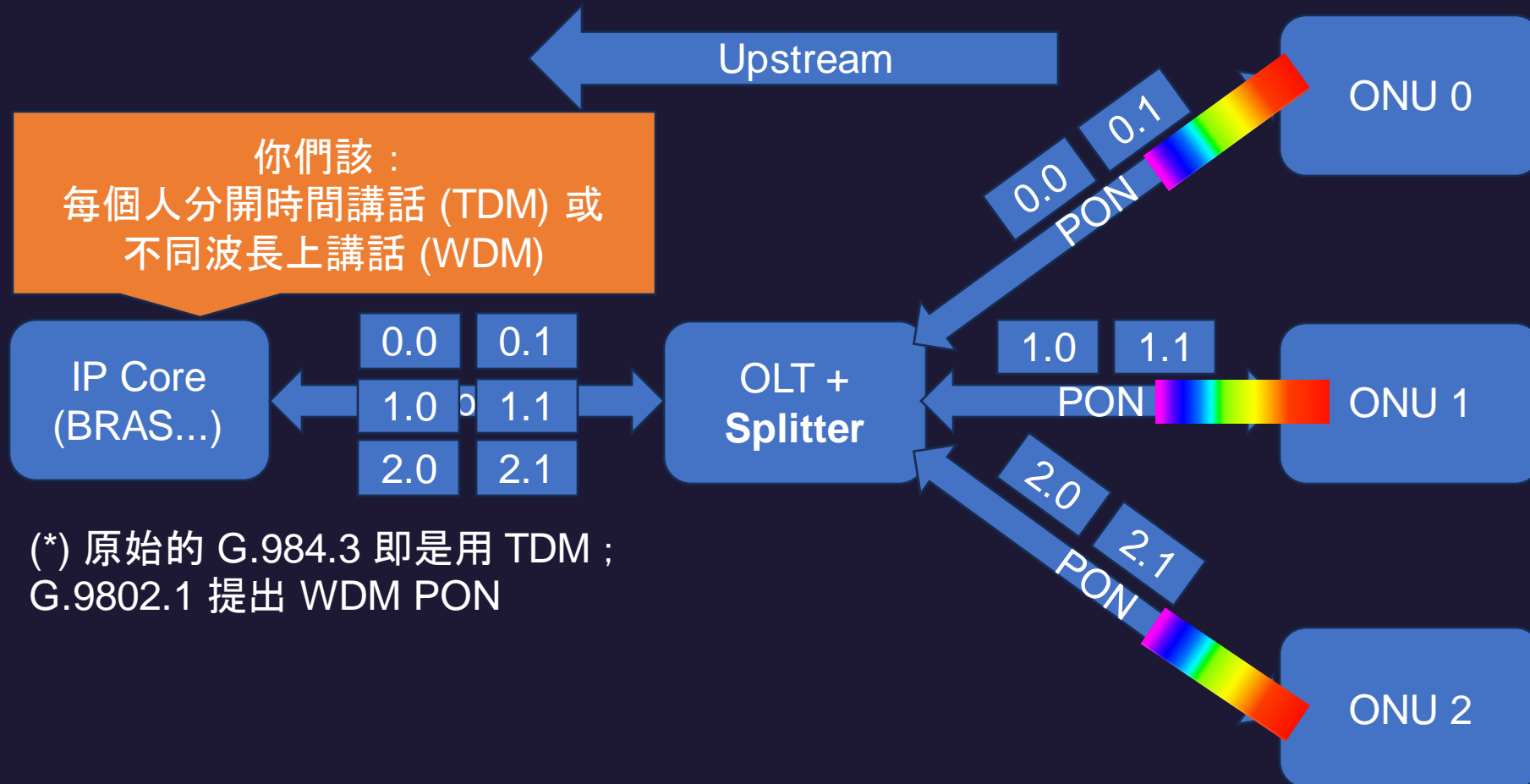
PON Transport Security (§12, ITU-TG.984.3)



PON Transport Security (§12, ITU-TG.984.3)

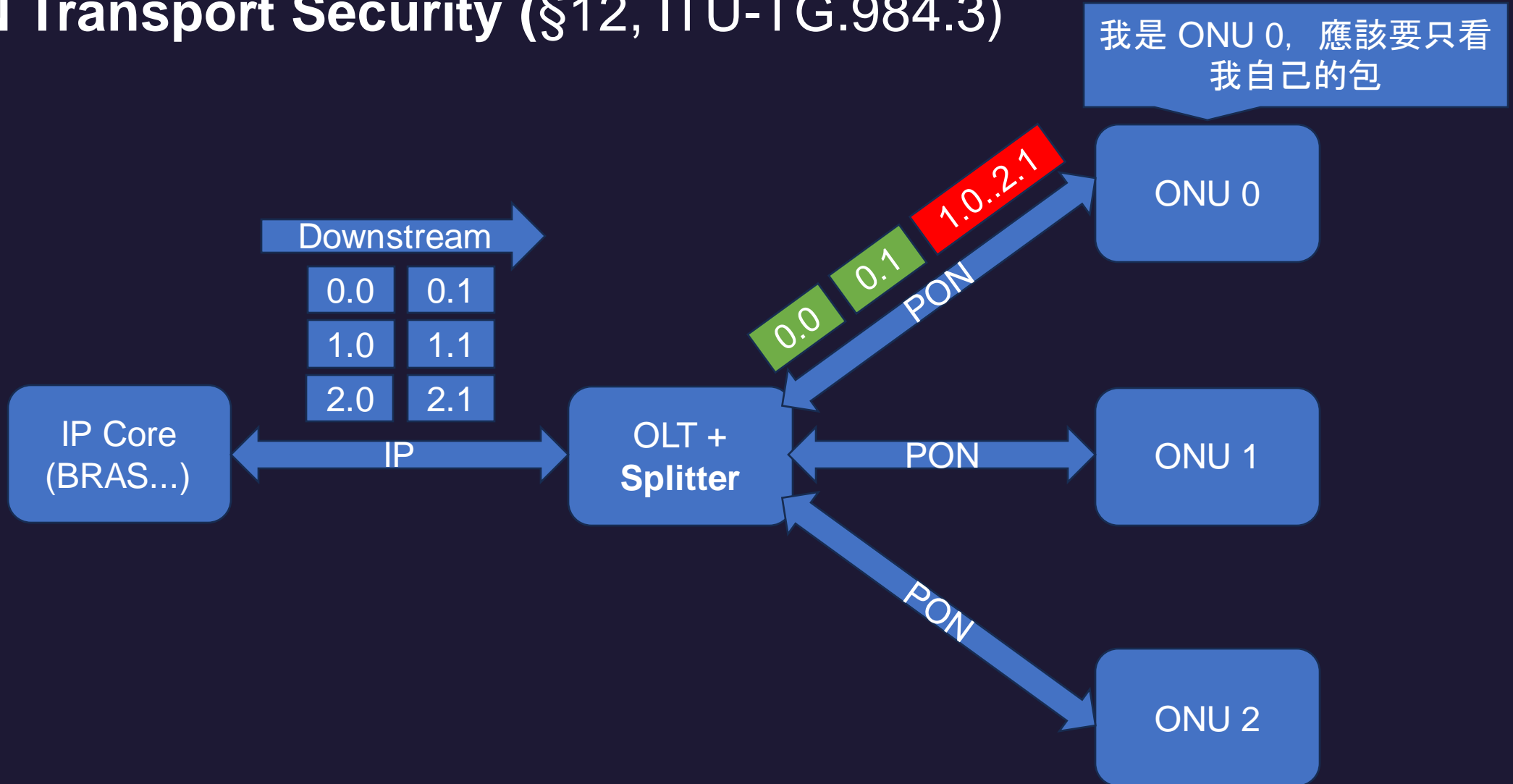


PON Transport Security (§12, ITU-TG.984.3)

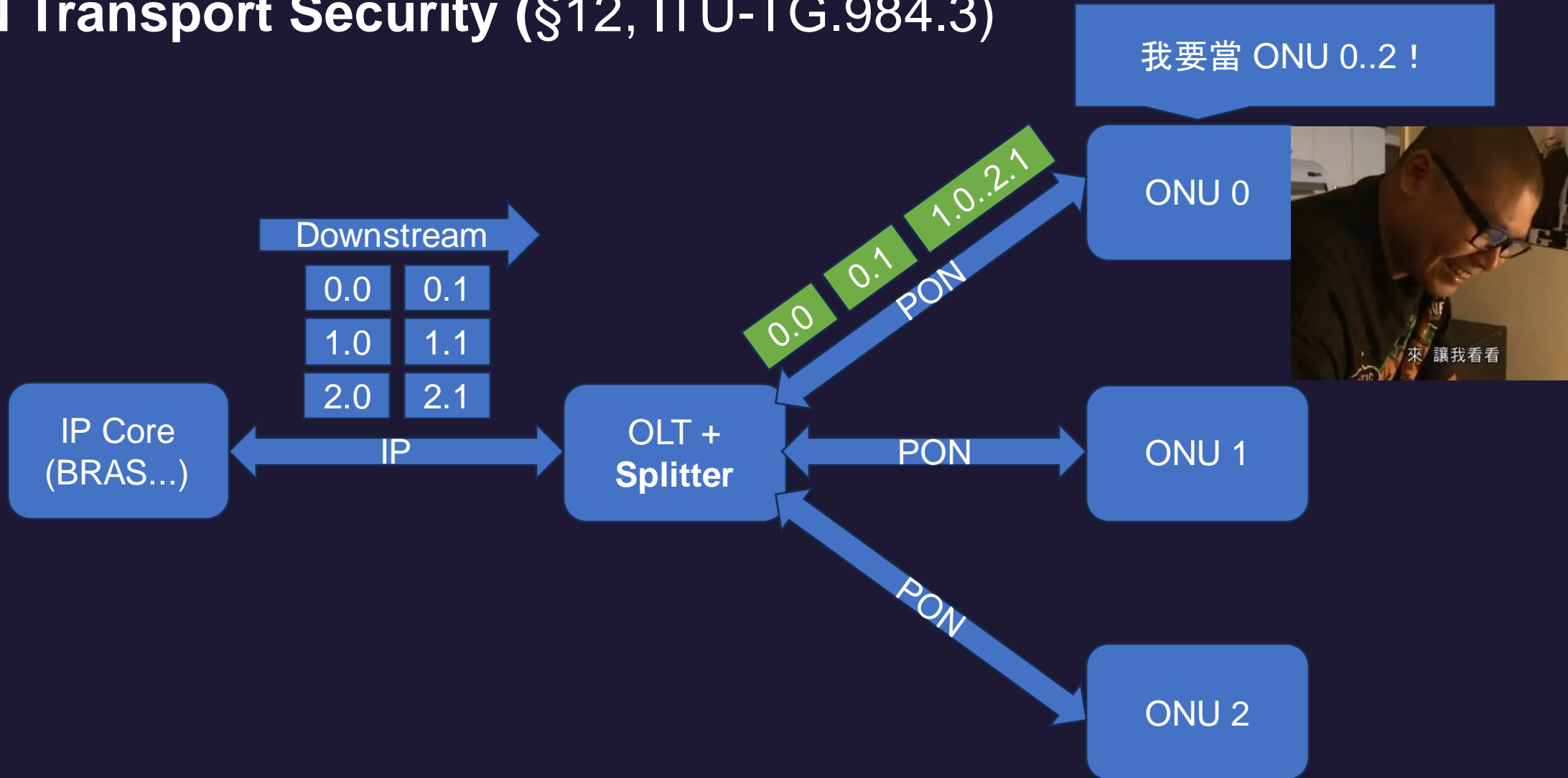


(*) 原始的 G.984.3 即是用 TDM ;
G.9802.1 提出 WDM PON

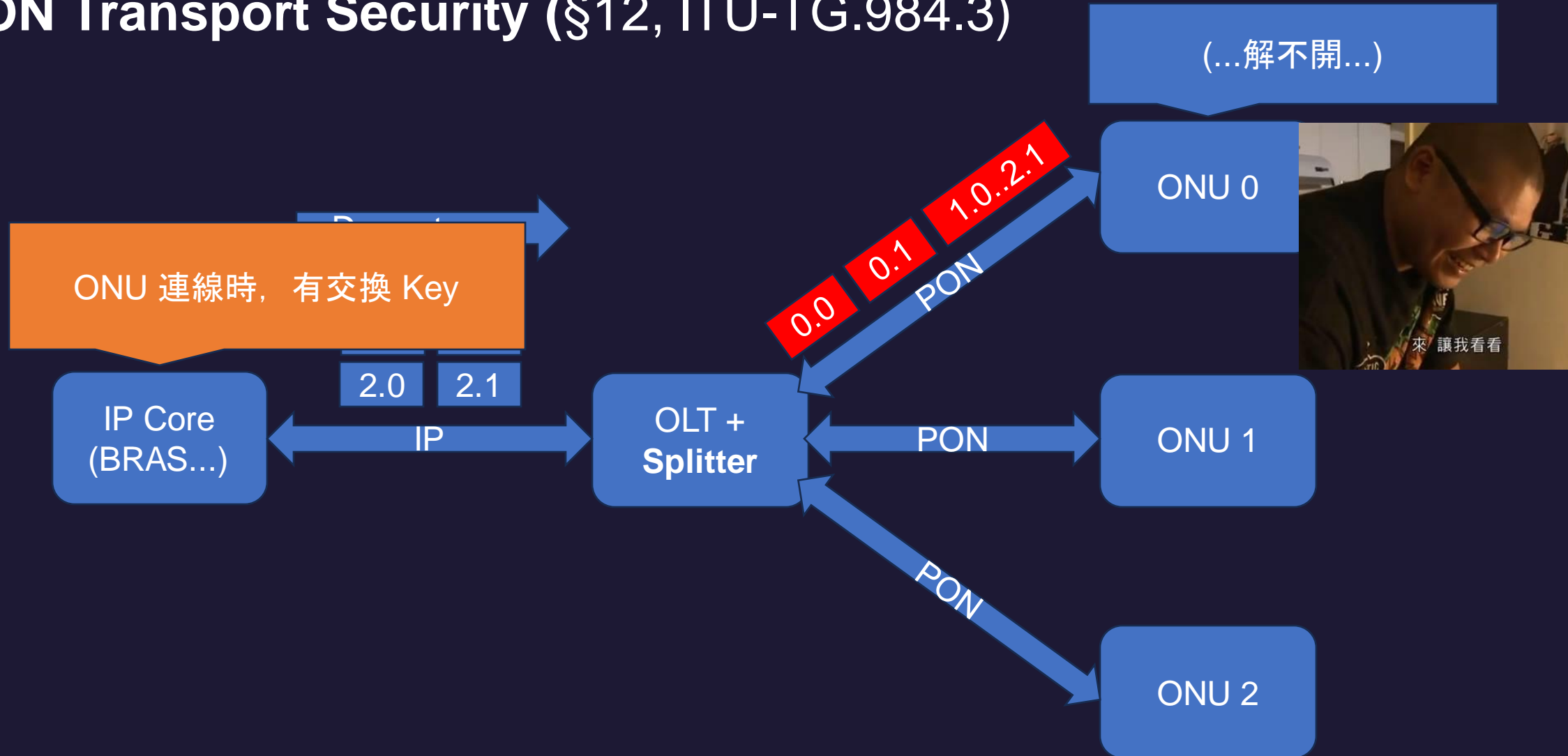
PON Transport Security (§12, ITU-TG.984.3)



PON Transport Security (§12, ITU-TG.984.3)



PON Transport Security (§12, ITU-TG.984.3)



Wiretapping

- **Passive Optical Network: 被動光纖網路**
- **Splitter = 菱鏡**
- **只要最終的光線強度足夠，就可以收發**
 - 副作用：電信公司通常會偵測強度降低等問題
- **只有 Downstream 加密**



設備角度 — GPON FTTH 架構

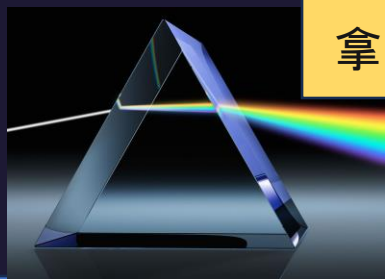
攻擊來源 (Internet/ISP)

IX

拿下 OLT/Core, 可控制傳輸內容或路由



拿下 ONU/CPE, 可控制單一 Subscriber



ONU/CPE

Base-band

Router

攻擊來源 (User)

User PC

IP Core (BRAS...)

OLT

PON

Splitter

PON

IP, Copper

IP

IP

IP

OLT

...

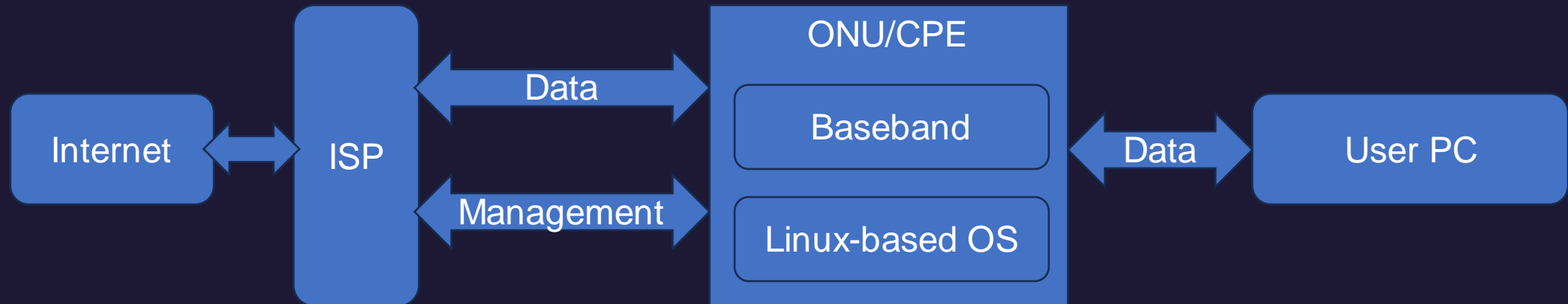
PON

ONU/CPEs...

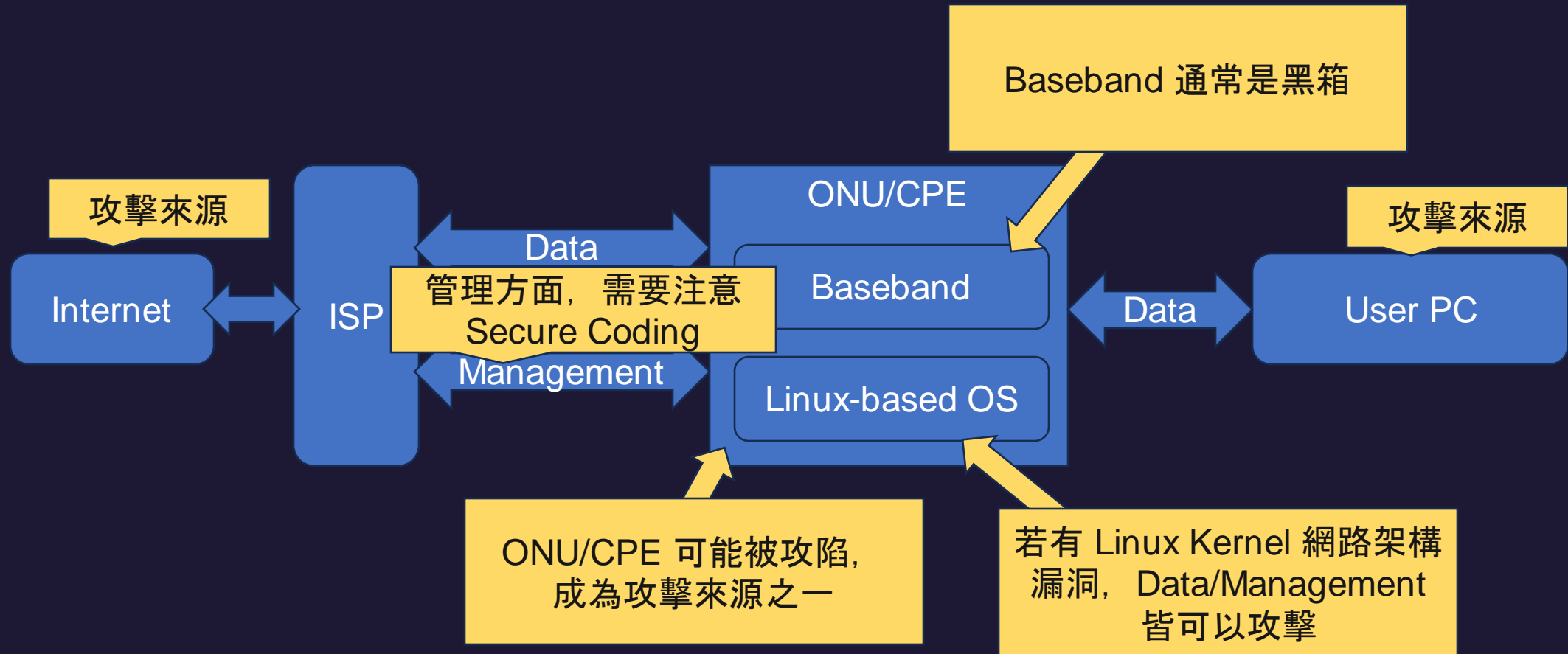
OLT

...

ONU/CPE 攻擊面角度



ONU/CPE 攻擊面角度



管理面角度

ISP 需要管理眾多終端設備

混亂邪惡

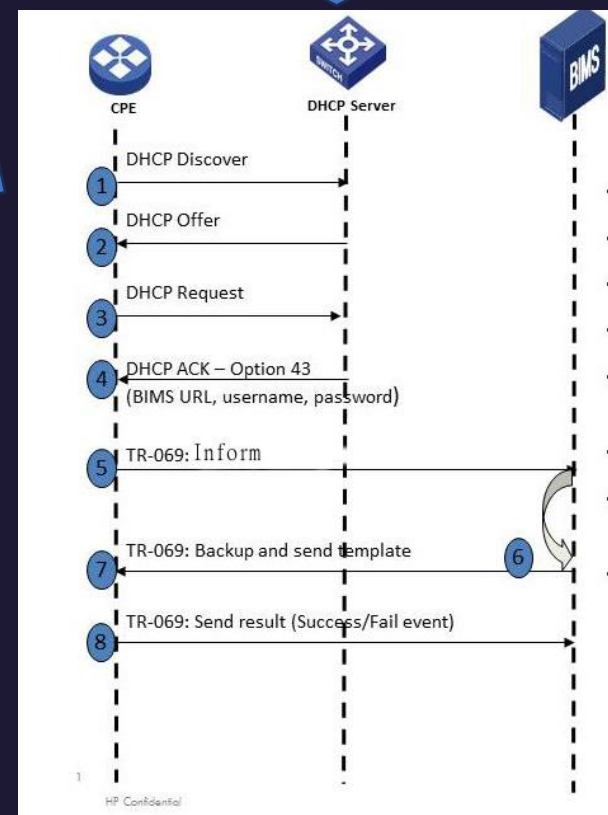
大家用的方法

TR-069 是由 CPE 主動發起，無須開放外部連線。

```
iptables -A INPUT -p tcp -s <isp> --dports 22,443 -j ACCEPT
```

(*) 不代表好壞，兩種用法全球皆有

Further, [redacted] is a proprietary protocol and it is assumed that all the devices in the network are of the same kind and do not expect any interoperability with other devices (in the market). Our internal team may, if required, post further comments in appropriate forums. BR, [redacted]



(*) 其實還是需要 `iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT`

著手分析 ONU/CPE

外鄉打法—OSINT、入手硬體和韌體

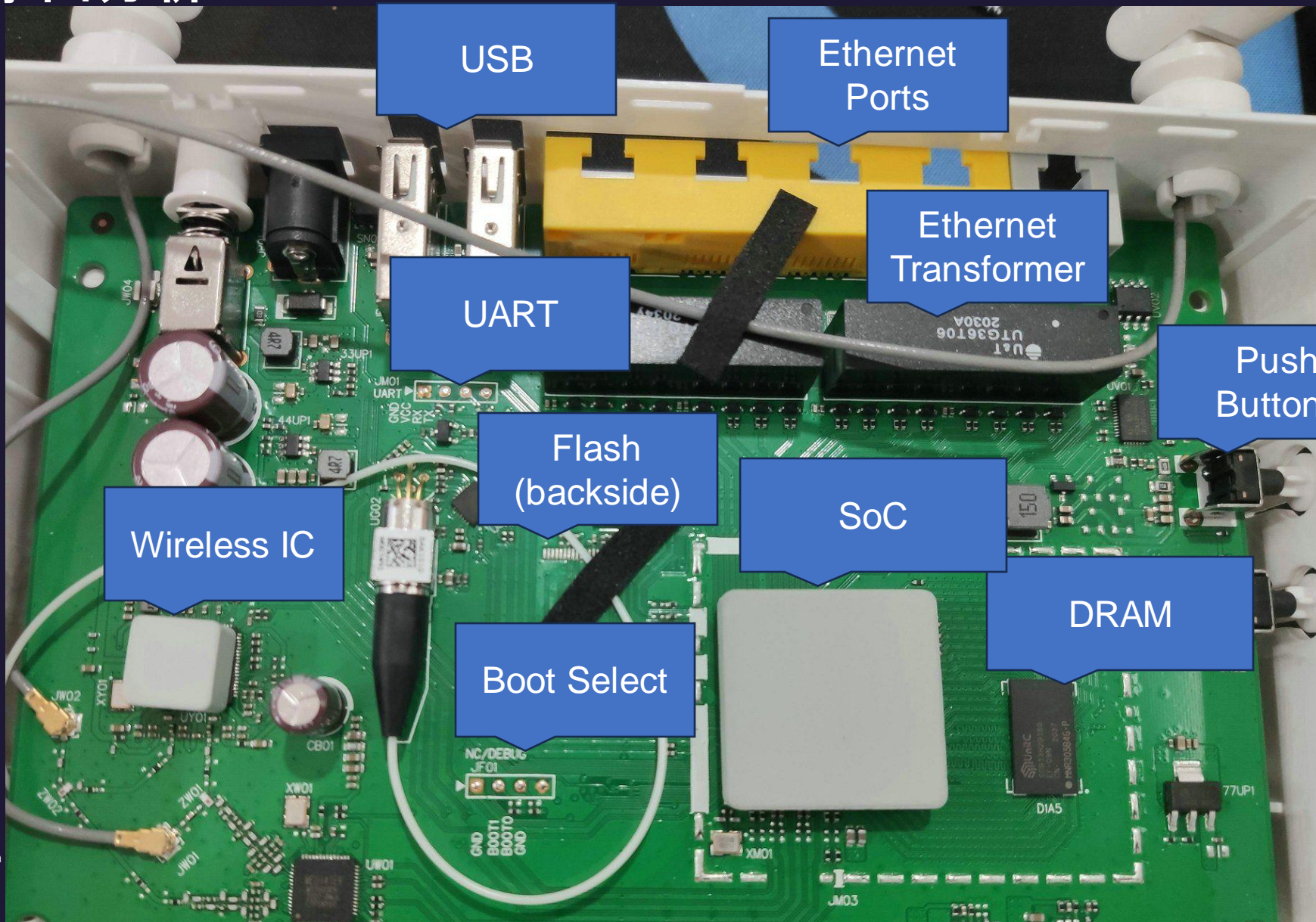
- Google:// 會找到：
 - 韌體
 - PCB 分析
 - 管理帳號密碼
- 硬體：
 - 大部分數據機硬體是 ISP 擁有
 - 試試買斷



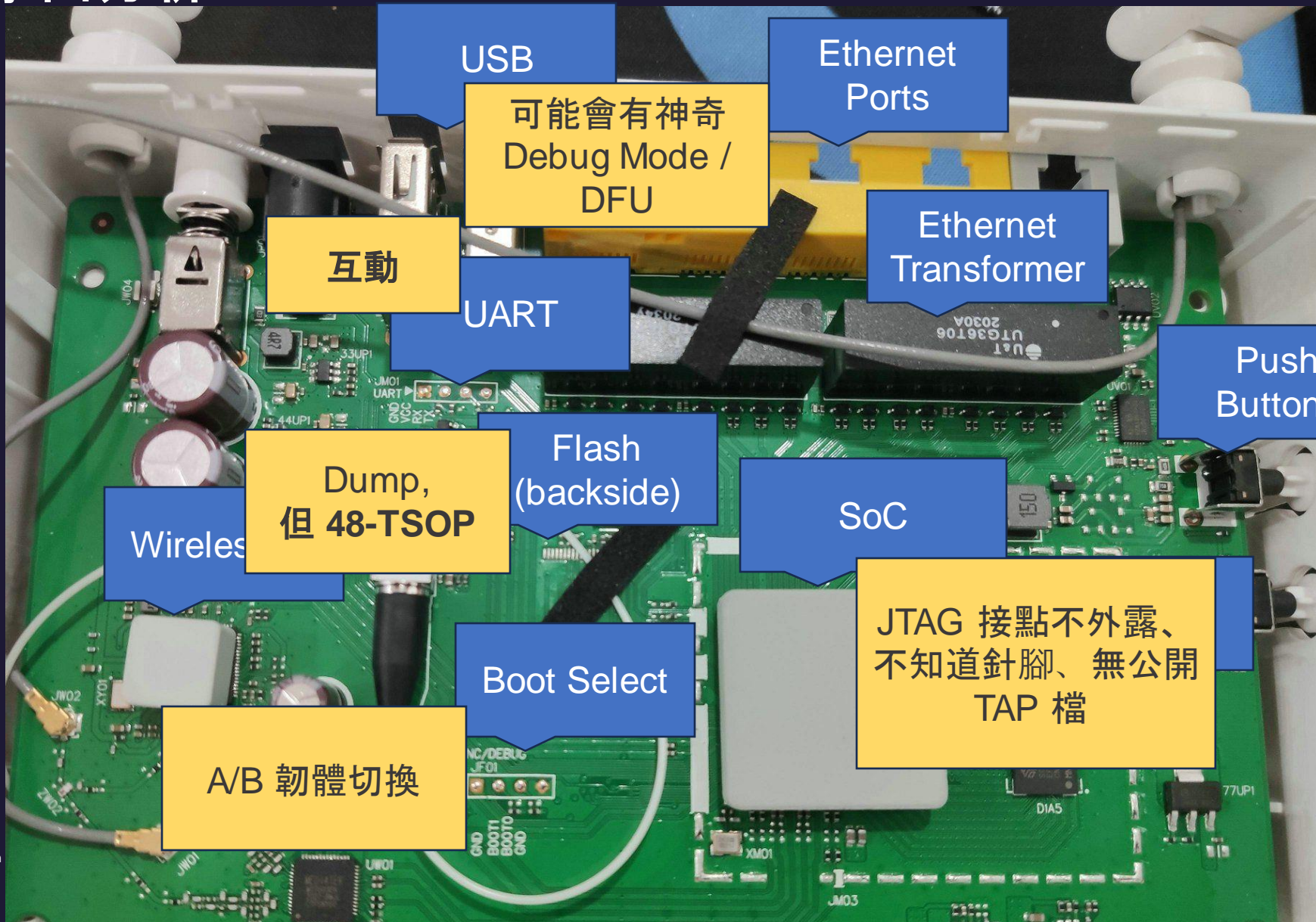
硬體分析的需求

- 目標：取得更多攻擊網路架構或 ISP 的資料
 - 取得設定值
 - 取得韌體
 - 取得暫時性 Shell

硬體攻擊面分析



硬體攻擊面分析



USB

Ethernet Ports

可能會有神奇
Debug Mode /
DFU

互動

Ethernet
Transformer

UART

Push
Buttons

Dump,
但 48-TSOP

Flash
(backside)

SoC

Wireless

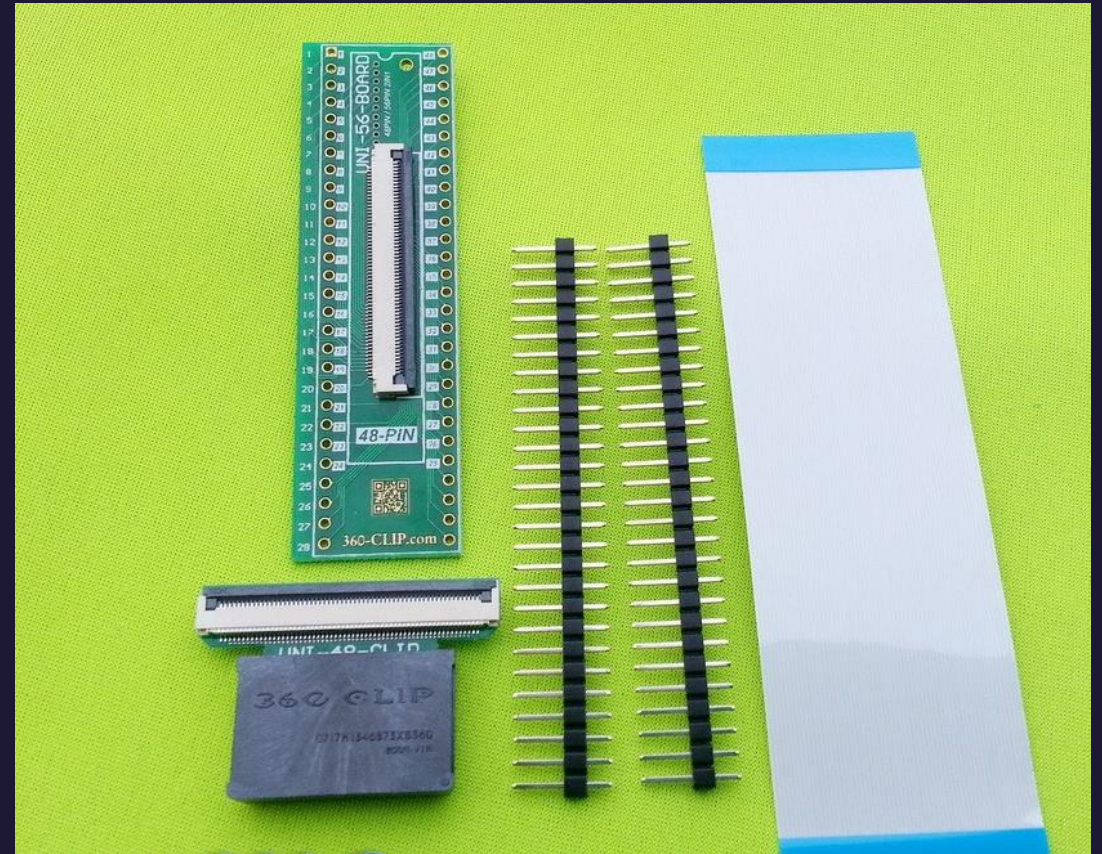
JTAG 接點不外露、
不知道針腳、無公開
TAP 檔

Boot Select

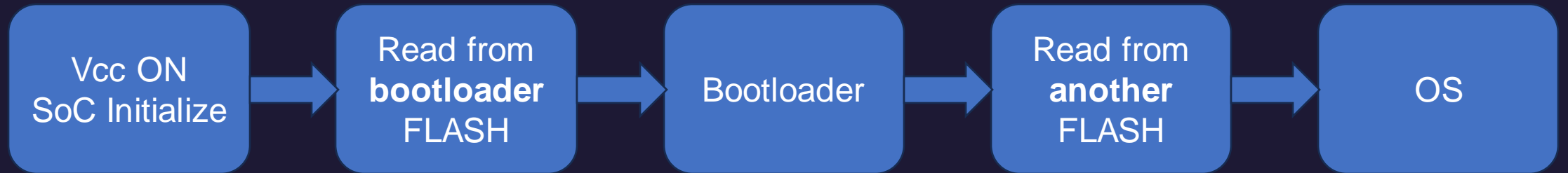
A/B 韌體切換

靠天，是 48-TSOP

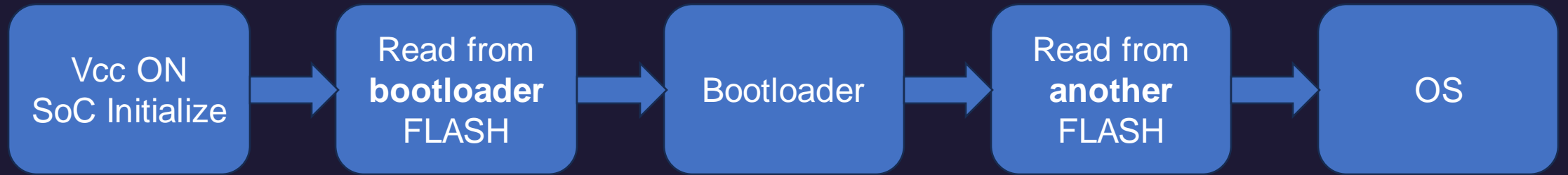
- Pitch 0.5mm - 5 根頭髮
- 解焊有風險
 - 全世界只有一家有賣 clip
- 目標是 Raw NAND，要處理 flash page



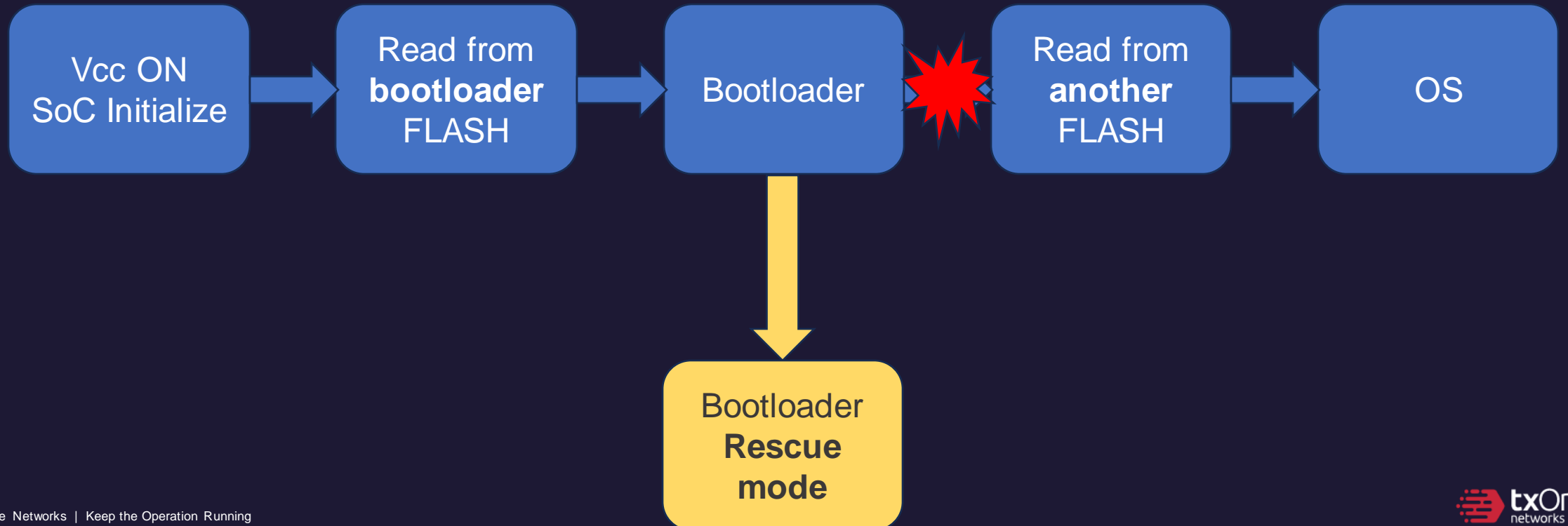
開機流程



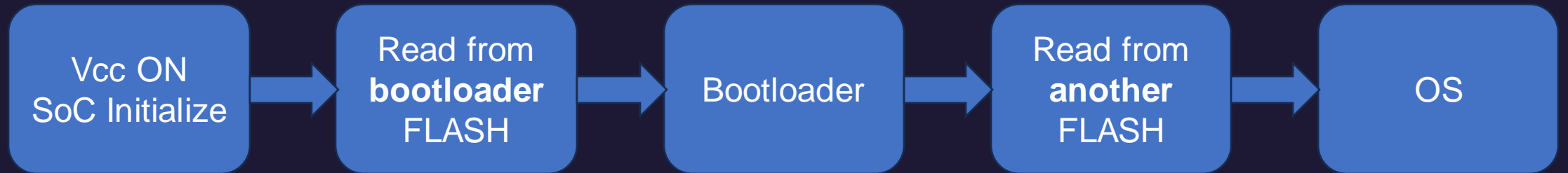
開機流程



開機流程



開機流程

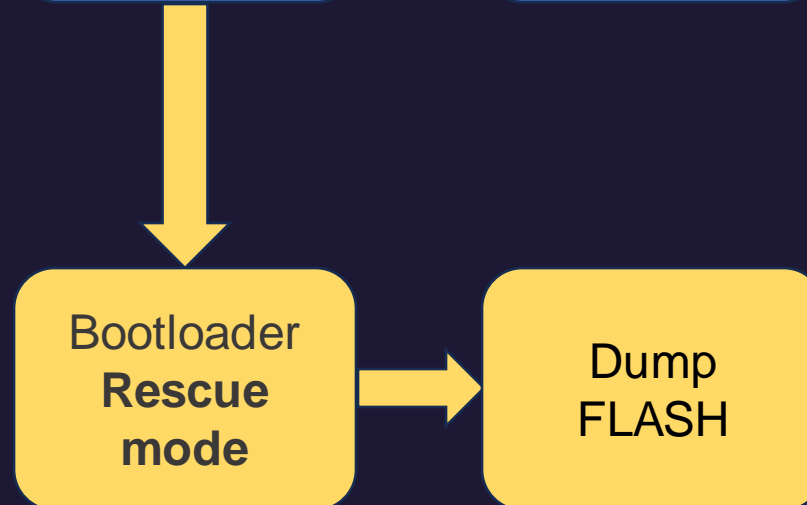


```
COM8 - PuTTY
SDRAM: Calibrating PHY
SEQ.C: Preparing to start memory calibration
SEQ.C: CALIBRATION PASSED
SDRAM: 1024 MiB
ALTERA DWMCMC: 0

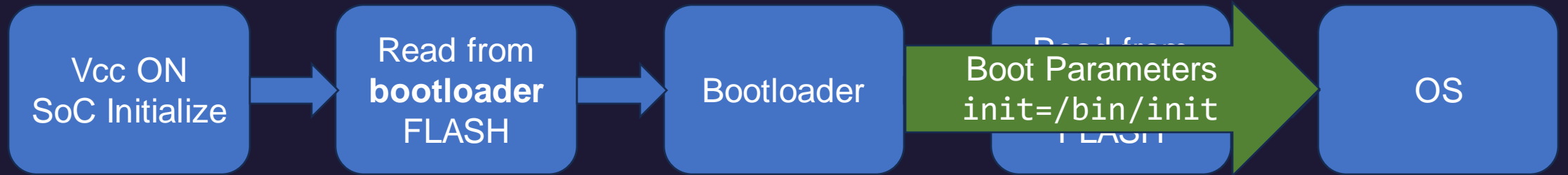
U-Boot 2013.01.01 (Aug 08 2014 - 10:46:23)

CPU : Altera SOCFPGA Platform
BOARD : Altera SOCFPGA Cyclone V Board
I2C: ready
DRAM: 1 GiB
MMC: ALTERA DWMCMC: 0
In: serial
Out: serial
Err: serial
Skipped ethaddr assignment due to invalid EMAC address in EEPROM
Net: mii0
Warning: failed to set MAC address

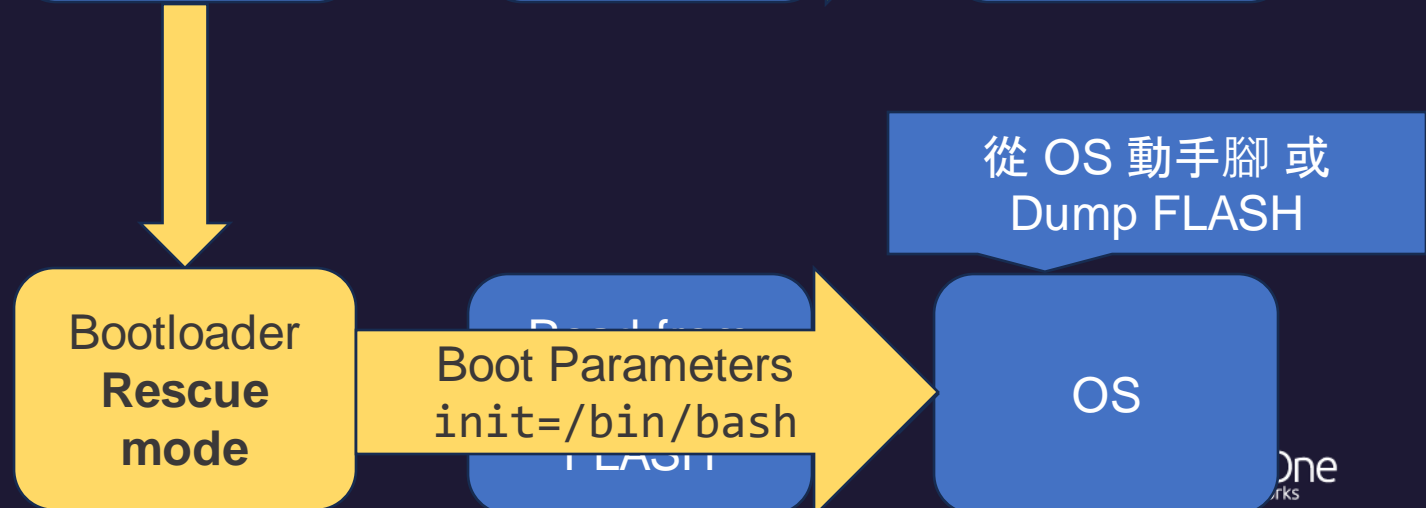
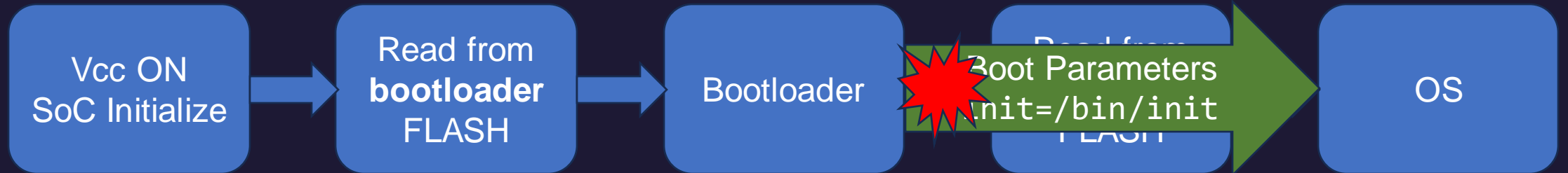
Hit any key to stop autoboot: 0
SOCFPGA_CYCLONE5 #
```



開機流程



開機流程



```
COM8 - PuTTY
SDRAM: Calibrating PHY
SEQ.C: Preparing to start memory calibration
SEQ.C: CALIBRATION PASSED
SDRAM: 1024 MiB
ALTERA DWMCMC: 0

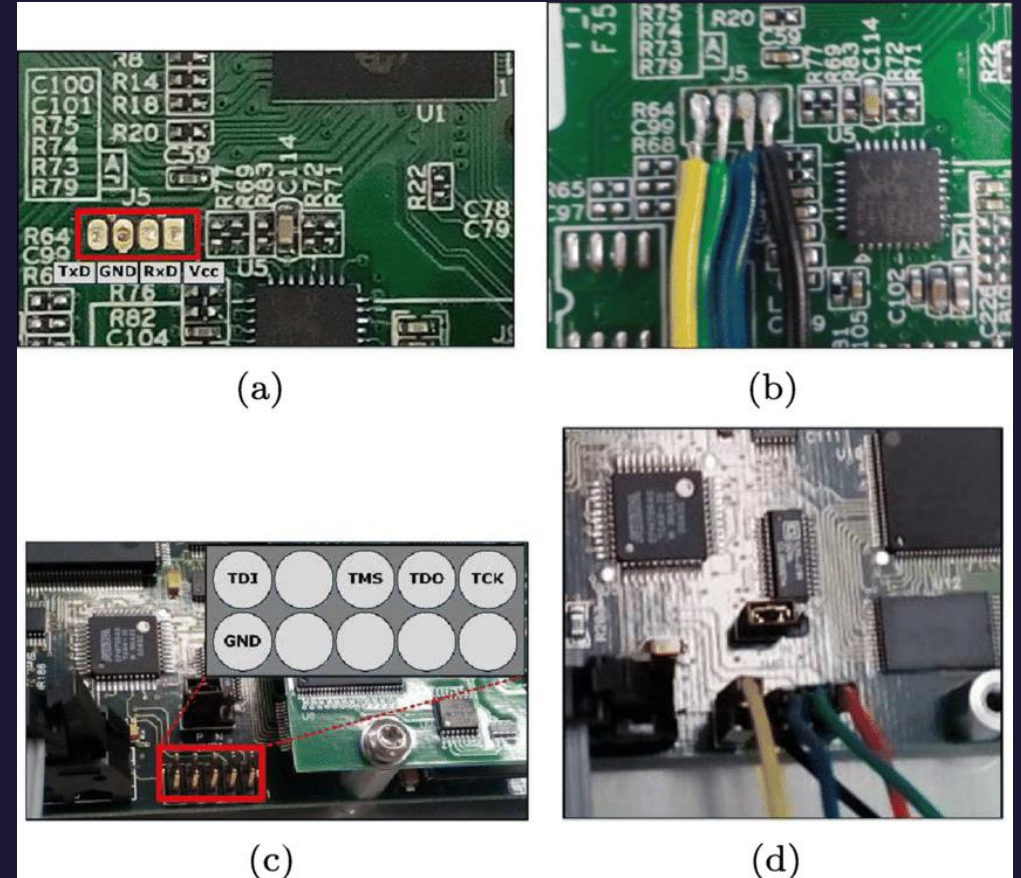
U-Boot 2013.01.01 (Aug 08 2014 - 10:46:23)


CPU : Altera SOCFPGA Platform
BOARD : Altera SOCFPGA Cyclone V Board
I2C: ready
DRAM: 1 GiB
MMC: ALTERA DWMCMC: 0
In: serial
Out: serial
Err: serial
Skipped ethaddr assignment due to invalid EMAC address in EEPROM
Net: mii0
Warning: failed to set MAC address

Hit any key to stop autoboot: 0
SOCFPGA_CYCLONES #
```

快速找出 UART/Debug 位

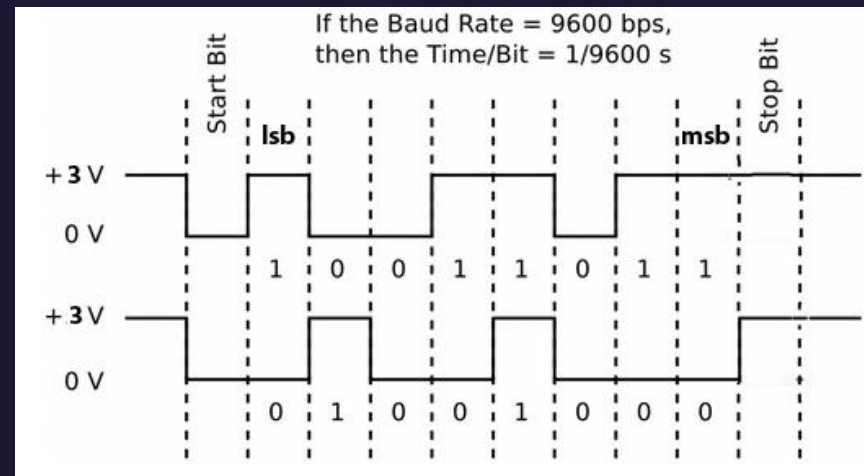
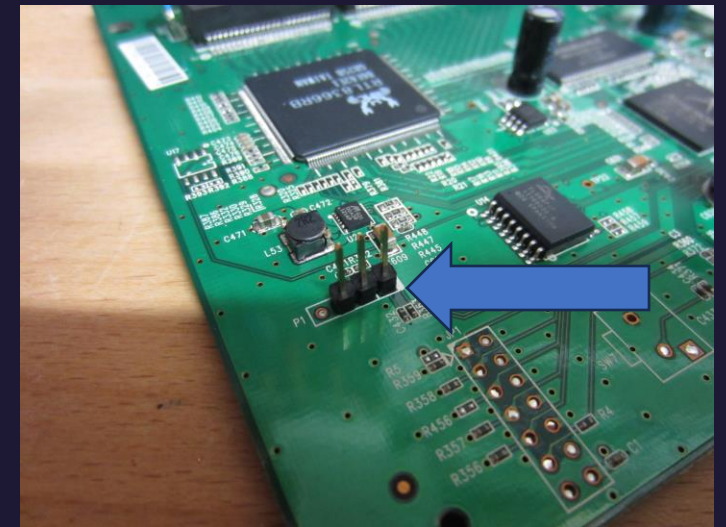
- 工具：
 - 一台高階（快）的電錶
 - 或 Logic Analyzer
 - PCBite + 兩雙手
- 如果 SoC 並非常見，
不要浪費時間在 JTAG



*Konstantinou, Charalambos & Maniatakos, Michail. (2019). Hardware-Layer Intelligence Collection for Smart Grid Embedded Systems. Journal of  txOne Hardware and Systems Security. 3. 10.1007/s41635-018-0063-0.

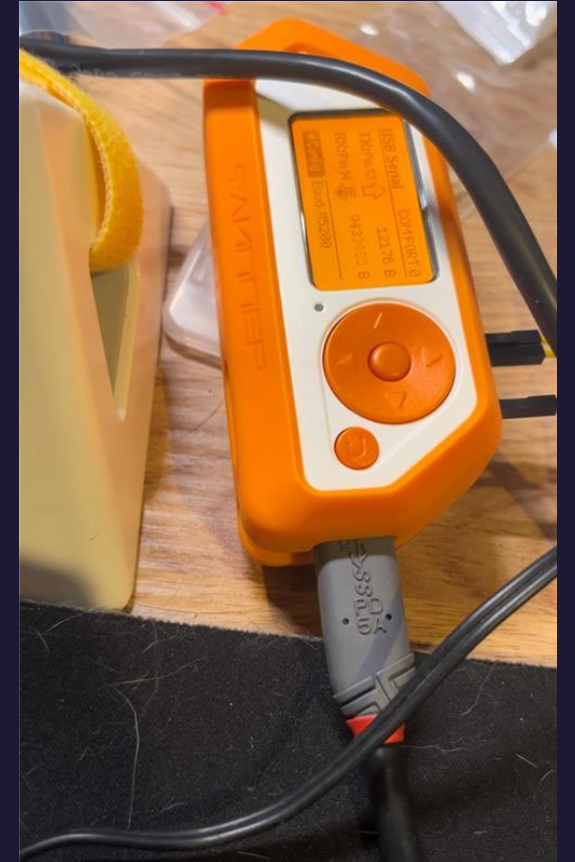
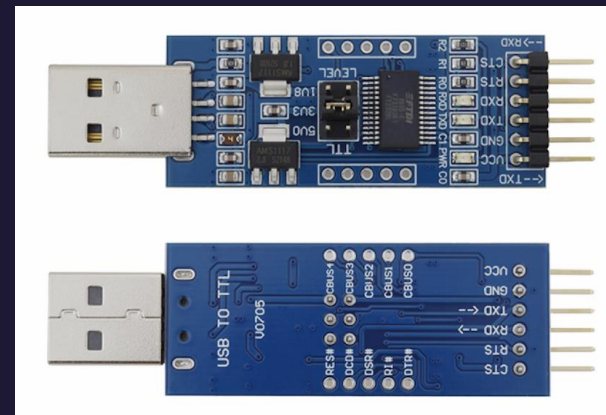
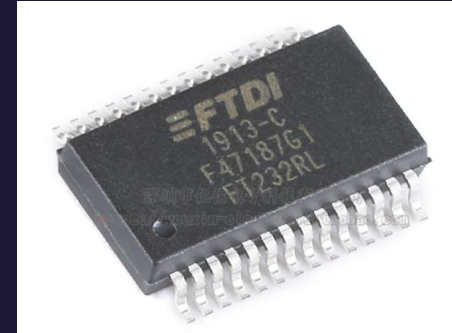
焊接！

- UART 通常是 3.3/5v
 - 開機時發現會 $\uparrow\downarrow\uparrow\downarrow$ ，又是四根腳，
大概都是 UART
- 焊不上去？
 - 板子通常都是多層板、GND Plane 通常很大塊
 - 遮罩通常都是 GND！



UART-USB 的選擇

- 常見：
 - FTDI FT232(H)
 - CP2102
 - Flipper Zero
- 小心低價劣質仿冒品



Got UART!

```
Base: 4.8_01
CFE version 1.0.38-116.233 for BCM96848 (32bit,SP,BE)
Build Date: Wed Mar 20 23:08:57 CST 2019 (ci@builder)
Copyright (C) 2000-2013 Broadcom Corporation.

Boot Strap Register: 0x10000000
Chip ID: BCM68488_A1_, MIPS: 600MHz, DDR: 533MHz, Bus: 300MHz
RDP: 428MHz
Main Thread: TP0
Total Memory: 268435456 bytes (256MB)
Boot Address: 0xb8000000
```

Bootloader shell to dump

CFE = Common Firmware Environment (by Broadcom)

```
CFE> help
Available commands:

m          Load manufacturing factory defaults
v          Display cfe & application firmware version(s).
x          Change extra partitions size
...
dm         Dump memory or registers.
db         Dump bytes.
dh         Dump half-words.
dw         Dump words.
w          Write the whole image start from beginning of the flash
dn         Dump NAND contents along with spare area
```

Bootloader shell to dump

```
CFE> dn 0x8700000 0
----- block: 984, page: 0 -----
08700000: 55424923 01000af8 9cd73513 00000004  UBI#.....5.....
08700010: 00000282 00008180 00000000 00006000  .....` .
08700020: 41414141 41414141 41414141 41414141  AAAAAAAAAAAAAAAAAA
08700030: 00000ab4 00000ab4 00000000 981971e3  .....q.
```

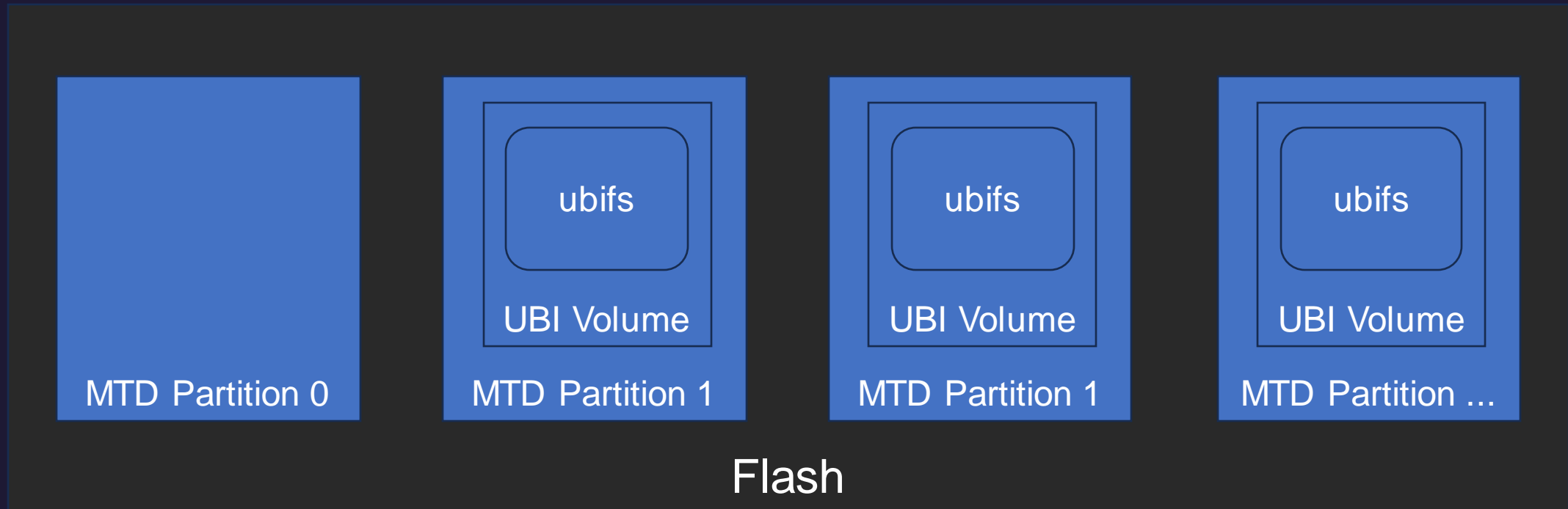
Flash dumping time!

- <https://github.com/depau/bcm-cfedump>

```
CFE> dn 0 0 1 # dn {block} {page} {page at a time}
CFE> dn 0 1 1
CFE> dn 0 2 1
...
```

- 驚人的 **115200** baud (約 1KiB/秒...)
- Flash 2GB = **23 days**

UBI



Helpful boot messages

- 我們有興趣的：rootfs, data

```
Creating 13 MTD partitions on "brcmnand.0":  
 0x000003280000-0x0000060e0000 : "rootfs" -> 105344KiB  
...  
 0x000006400000-0x000006800000 : "data" -> 4096KiB
```

- 23 days -> 1.3 days

Firmware extraction

- UBI 實作有一些 quirks
 - binwalk -e 不一定可以用
 - 建議 <https://github.com/nlitsme/ubidump>
- 終於有 rootfs 了

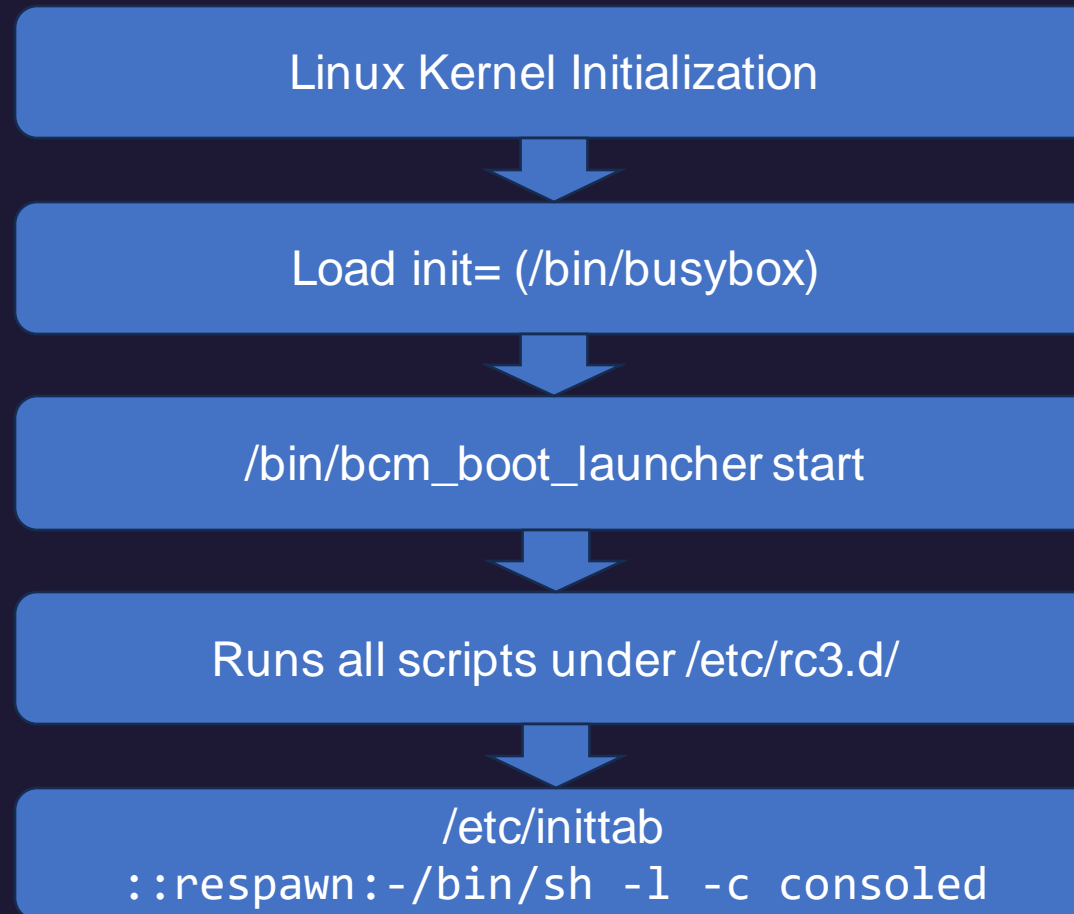
```
$ ls rootfs-fix/ubifs-root/rootfs-fixed.img/squashfs-root/  
bin  data  debug  etc  log  opt  sbin  tmp  var  
Data dev  lib    mnt  proc sys  usr
```

韌體架構分析

- 分析軟體/網路層組成、SBOM、實作
- 取得一些金鑰



Post-OS Init

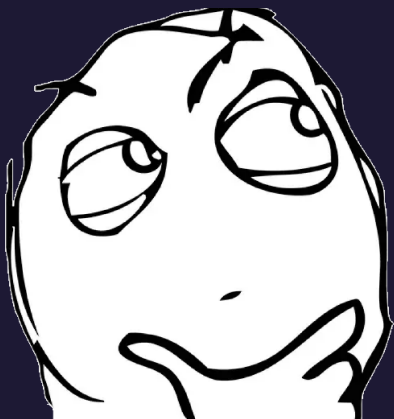


```
TargetModem Login: root
Password:
Login incorrect
```

Post-OS Init

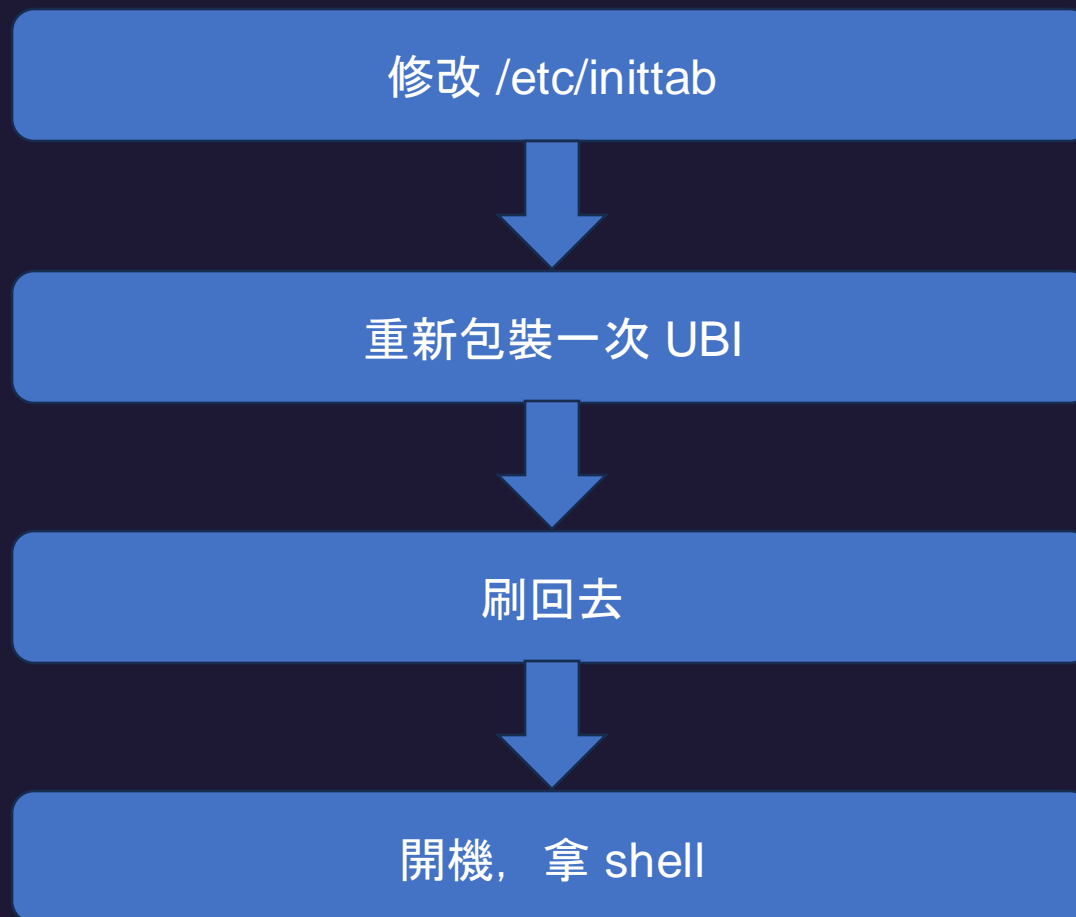
```
$ cat /etc/inittab
# This file contains customizations for the Broadcom CPE Router SDK

# if you don't want to type username/passwd in console login, copy this
# file to inittab.custom and replace "-/bin/sh -l -c consoled" below with "-
/bin/sh"
# The '-' means interactive, is still attached to terminal
::respawn:~/bin/sh -l -c consoled
```



- 目標機的分割區都是 ro (squashfs)
- 目標沒有 Root-of-Trust
- 可以用 CFE 寫任意 NAND...

狂野取 Shell 流程



狂野取 Shell 流程

修改 /etc/inittab



重新包裝一次 UBI

```
Broadcom Traffic Ordering Agent -- starting on w10 as daemon process...  
--BOOT DONE--
```

```
BusyBox v1.27.2 (2020-12-07 11:21:55 CST) built-in shell (ash)  
Enter 'help' for a list of built-in commands.
```

```
# whoami  
/bin/sh: whoami: not found
```

開機，拿 shell

取得一些金鑰

- ONU/ONT 認證 (from ITU-TG.984.3)
 - ONU/ONT 預先設定好 **SLID**, 再連線到 OLT
 - 或 : Core 以 Device ID 去分配 **SLID** 給每一台 ONU/ONT

```
$ cat ./extracted/data/id  
<my house's SLID>
```

- 發現一組可以登入 consoled 的帳號密碼, 白忙了

```
$ cat /etc/shadow # 內容可以 hashcat 輕鬆解出
```

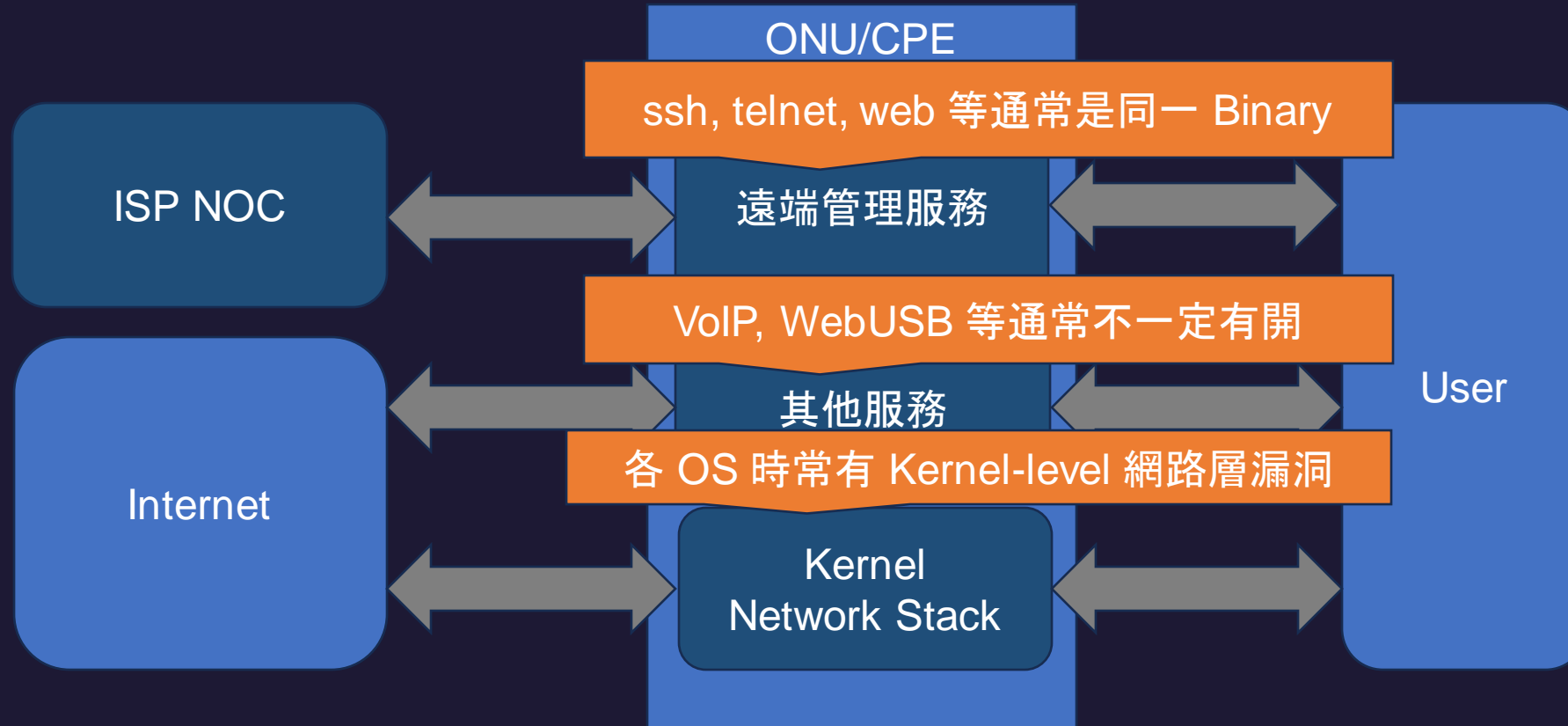
網路攻擊面分析

- 交叉比對 iptables + ps

```
Chain [redacted]
target prot opt source destination

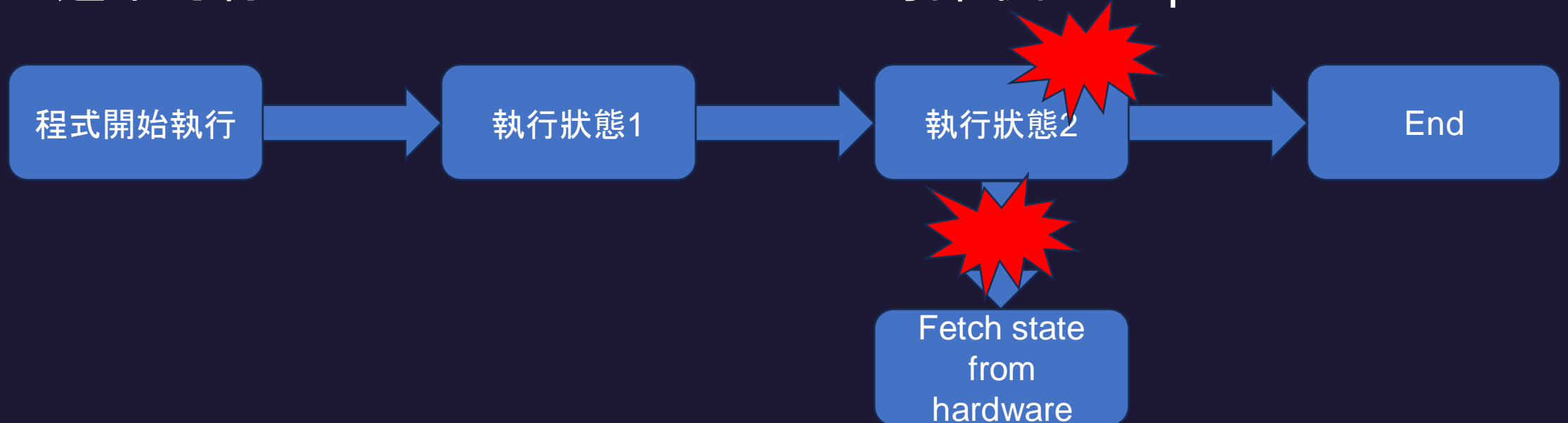
# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 127.0.0.1 0.0.0.0:* LISTEN [redacted]
tcp 0 0 127.0.0.1 0.0.0.0:* LISTEN [redacted]
tcp 0 0 127.0.0.1 0.0.0.0:* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
tcp 0 0 :::* :::* LISTEN [redacted]
```


GPON modem 常見網路攻擊面



測試管理服務/其他服務

- arm-based 目標無法輕易 qemu-system, 需要逐一在 QEMU 上實作, 或是需要某程度 patch
- 通常可行 : Network-based fuzzer / 局部取出並 qemu-static



<https://www.thezdi.com/blog/2020/5/27/mindshare-how-to-just-emulate-it-with-qemu>

Fuzzing 好用，但不一定需要

- 不少比例漏洞，都不一定需要 Fuzzing 找出
- 需要對不同 Layer 之間有相當了解
 - Kernel<->User, L2<->L3<->L4<->L7...

用 vim 找到的 (vim + scapy)

HITCON PEACE 2022 CYBER WAR

如何(不)讓你發射飛彈

Disrupting factories, missile bases and warships –
Exploration into DDS protocol implementations

Ta-Lun Yen
Federico Maggi
Erik Boasson
C. Toyama, P. Kuo, and M. Cheng
Victor Mayoral Vilches

TXOne Networks
Trend Micro Research
ADLINK
TXOne Networks
Alias Robotics

txOne networks

...種種網路設備上常發現的問題

• 軟體問題

- 沒有權限區分
 - 全部服務都是 UID 0
- 沒有 ASLR / PIE / Stack Canary
- Secure Coding Issues
 - 常見命令注入、BoF...
- 常見的 Crypto 實作 issues
 - 1DES、Fixed key、IV reuse...
- 老舊 Kernel
- 後門帳號

• 硬體問題

- 過度開放的 Debug Port
- 沒有 Root-of-Trust
- 沒有 Secure Boot
- 沒有韌體驗證機制
- SoC/SDK 過度老舊
- ...

Conclusions

我們應該要朝更安全的方向走嗎？



朝更安全的方向走

- 網路設備安全應該跟上時代的腳步
- 應該使用較新、有 Root-of-Trust 的 SoC
- 應該更徹底的有 Secure Coding 概念
- 實作最小權限概念、永遠預設產品活在惡意環境當中

未來期許

- 增加對於資訊安全的投資
- 設計更安全的協定與軟硬體架構
- 增加承受系統性風險的韌性

Questions?

- talun_yen@txone.com
- twitter.com/evanslify
- 請密切專注我們後續發表