Internal
Discussion

Edge Router Network Data Analysis and Machine Learning

Chen-Hao Hsiao, Yu-Cheng Hsiao, Hsin-Ray Yang, Wen-Shao Ho
I-Hsiang Wang
National Taiwan University
2022/04/26

Outline

- Recap
- WIFI#3-1案例討論
- 異常偵測

PART I. Recap

分群結果

- 針對 AIMESH#MASTER 做 clustering，共有2517 筆資料 model 。
- 拿掉 customer 以及 wifi#1,wifi#5 等 tags 後,剩下 77 個 tags 。
- 主要分群依據來自 CRASH#7, CRASH #9, CRASH #11, REBOOT#3, SPEED#1 這 5 個 tags。

Trival cluster (不含任何tag)	Crash#7 cluster	Complete cluster	CRASH#11	Crash#9_in cluster	REBOOT#3	Crash#9_out cluster
1359	220	344	137	219	126	112

討論:

1. CRASH#7, CRASH #9, CRASH #11, REBOOT#3,單獨存在比例高，可以當作是常見的現象？
   [ChengChe]**CRASH#7 pattern描述好像有誤? CRASH#9和CRASH#11現象明確但CRASH#11可能會有重複(因為feedback後檔案沒有被移除，導致新feedback會出現和舊feedback相同的檔案)**

1. 從 CRASH#9_in cluster 可發現有 CRASH #1, CRASH #4 時同時有 CRASH#9 的比例高,可以把 CRASH #4 和 CRASH#9 同時出現當作常見的現象

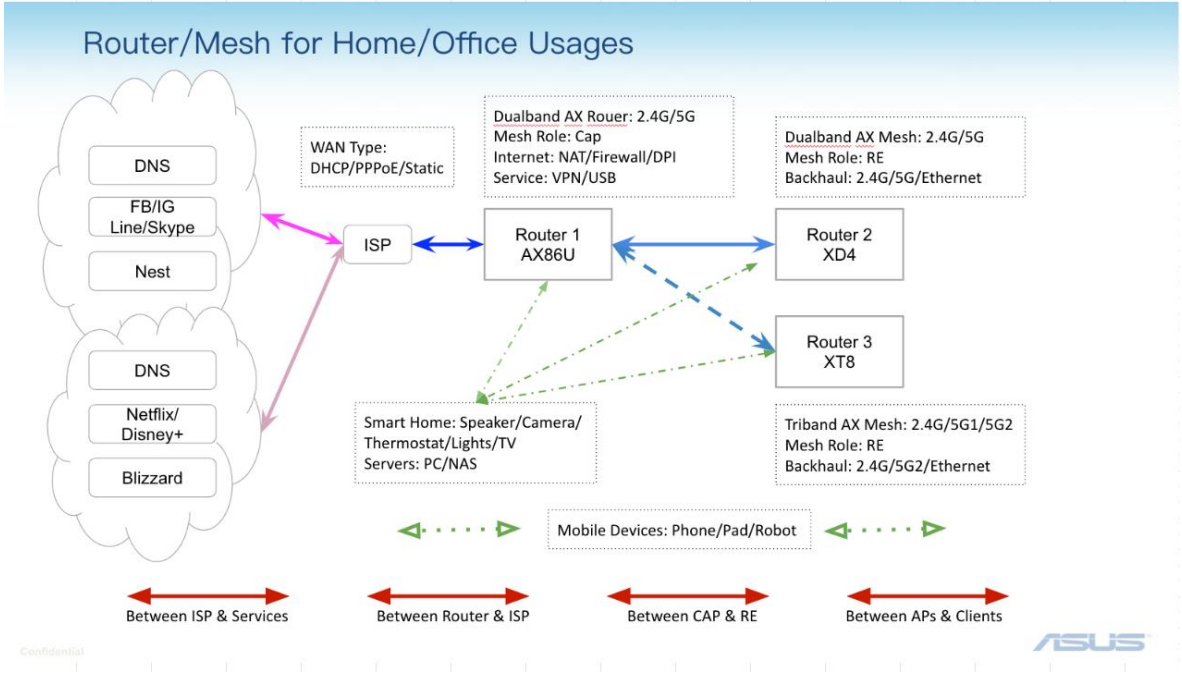
   [ChengChe]這點合理，CRASH#1和CRASH#9 的pattern重疊，CRASH#4的pattern也隱含在CRASH#9之中。

1. 同一群裡面的case 會不會都是發生類似的問題 (ex : Ob fial、no reason reboot、Unstable connection,...)，或者是從每一群的主要tags 能夠推論出 Router 可能是發生甚麼問題嗎？

根據上次結論，我們應該關注 *1)Router & ISP, 2)**CAP & RE** and 3)APs & Clients.*

目標是診斷出確切的異常現象。

討論: 每個tag對應的範圍(i.e. CAP-RE) 會不會有遺漏?



新資料(4/18)

“目前想法是希望從各案例為出發點，提供符合特定tag的案例。所以我這邊先更新 unstable connection 案例，符合WIFI#3-1標籤的案例（2G WIFI backhaul 持續10分鐘以上。）”

- **decice_connection.log：**裝置上下線log
  [2021-04-08 11:09:54][][D8:-:-:-:D2:0E] disconnect from [wl0.1]
  [2021-04-08 11:10:14][][D8:-:-:-:D2:0E] connect to [wl0.1]
- **backhaul_connection.log：**預期dual/tri band希望是持續連線在5G-1/5G-2/6G, 所以若某些原因跳至2G, 系統也會嘗試連回5G-1/5G-2/6G, 若持續10分鐘都沒連回就會標上WIFI#3-1
  [2021-04-08 11:42:49]Topology change from [init] to [2G]
  [2021-04-08 13:19:13]Topology change from [2G] to [5G/5G-1]
- **reboot.log：**系統開機log
  [2021-04-10 03:30:25]schedule system reboot
  [2021-04-11 03:30:28]schedule system reboot
- **process_crash.log:** process crash log

```
[2021-03-15 16:45:54]amas_wlcconnect crash
[2021-03-15 17:07:54]amas_wlcconnect crash
```

討論: 從Unstable connection(WIFI#3-1) 這種案例出發, 希望可以做到甚麼診斷?

WIFI#3-1	2G WIFI backhaul 持續10分鐘以上。	CAP - RE	analysis_topology_change_report	syslog.log

backhaul_connection.log

```
[2021-03-16 09:57:17]Topology change from [init] to [2G]
[2021-03-16 10:12:21]Topology change from [init] to [2G]
[2021-03-16 10:16:07]Topology change from [init] to [2G]
[2021-03-16 10:16:09]Topology change from [2G] to [init]
[2021-03-16 10:16:25]Topology change from [init] to [2G]
[2021-03-16 12:14:23]Topology change from [init] to [2G]
```

syslog.log

```
Mar 16 10:16:23 BHC: bandindex(0): state is 2
Mar 16 10:16:23 BHC: bandindex(1): state is 0
Mar 16 10:16:23 BHC: bandindex(2): state is 0
Mar 16 10:16:25 BHC: Topology change from -1 to 2.
Mar 16 10:16:32 kernel: CSIMON:  CSIMON[1.1.0] Initialization
```

```
Mar 16 12:14:23 rc_service: ntp 2423:notify_rc restart_diskmon
Mar 16 12:14:23 disk_monitor: Finish
Mar 16 12:14:23 disk_monitor: be idle
```

討論:同樣都是Topology change from[init] to [2G], 為甚麼對應到的 syslog.log 會不同？

process_crash.log

```
[2021-03-16 10:15:47]amas_wlcconnect crash
[2021-03-17 09:59:08]amas_wlcconnect crash
[2021-03-17 13:14:30]amas_wlcconnect crash
[2021-03-17 16:23:30]amas_wlcconnect crash
```

相同時間對應的syslog.log如下:

討論: 甚麼樣的情況會發生wlcconnect crash ?

```
Mar 17 09:59:08 rc_service: cfg_client 12667:notify_rc restart_wireless
Mar 17 09:59:08 kernel: CPU: 0 PID: 7552 Comm: amas_wlcconnect Tainted: P           O    4.1.52 #2
Mar 17 09:59:08 kernel: Hardware name: Generic DT based system
Mar 17 09:59:08 kernel: task: d27f4400 ti: cfc42000 task.ti: cfc42000
Mar 17 09:59:08 kernel: PC is at 0x146810
Mar 17 09:59:08 kernel: LR is at 0x1467b4
Mar 17 09:59:08 kernel: pc : [<00146810>]    lr : [<001467b4>]    psr: 800f0010
Mar 17 09:59:08 kernel: sp : bec277d8  ip : 00000000  fp : bec27ef4
Mar 17 09:59:08 kernel: r10: 001cd000  r9 : 00000000  r8 : 00000001
Mar 17 09:59:08 kernel: r7 : 00000000  r6 : bec27900  r5 : 00000000  r4 : 00000000
Mar 17 09:59:08 kernel: r3 : 00000003  r2 : ffffffff  r1 : 00000000  r0 : bec27900
Mar 17 09:59:08 kernel: Flags: Nzcv  IRQs on  FIQs on  Mode USER_32  ISA ARM  Segment user
Mar 17 09:59:08 kernel: Control: 10c5387d  Table: 0fccc04a  DAC: 00000015
Mar 17 09:59:08 kernel: CPU: 0 PID: 7552 Comm: amas_wlcconnect Tainted: P           O    4.1.52 #2
Mar 17 09:59:08 kernel: Hardware name: Generic DT based system
Mar 17 09:59:08 kernel: [<c0026fe0>] (unwind_backtrace) from [<c0022c38>] (show_stack+0x10/0x14)
Mar 17 09:59:08 kernel: [<c0022c38>] (show_stack) from [<c04bad5c>] (dump_stack+0x8c/0xa0)
Mar 17 09:59:08 kernel: [<c04bad5c>] (dump_stack) from [<c003ac6c>] (get_signal+0x490/0x558)
Mar 17 09:59:08 kernel: [<c003ac6c>] (get_signal) from [<c00221d0>] (do_signal+0xc8/0x3ac)
Mar 17 09:59:08 kernel: [<c00221d0>] (do_signal) from [<c0022658>] (do_work_pending+0x94/0xa4)
Mar 17 09:59:08 kernel: [<c0022658>] (do_work_pending) from [<c001f4cc>] (work_pending+0xc/0x20)
Mar 17 09:59:09 wlceventd: wlceventd_proc_event(508): eth4: Disassoc 04:-:-:-:17:20, status: 0,
reason: Disassociated because sending station is leaving (or has left) BSS (8), rssi:-57
```

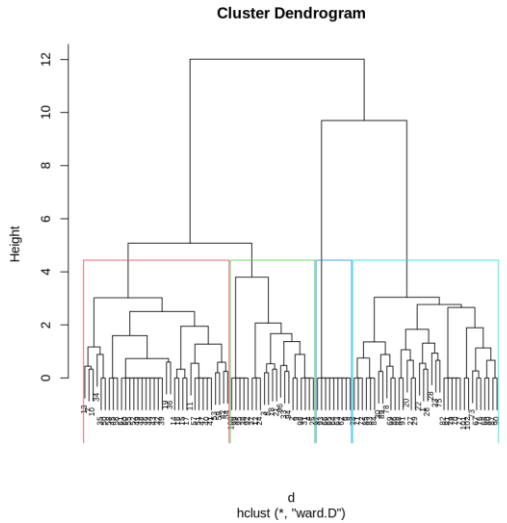
PART II. 分群結果說明

Hierarchical clustering on tags

- 針對有WIFI#3-1做 clustering

- 總共有102 筆資料
- 總共有 78 個 tags
- 全部都在RE，沒有在CAP上的資料

- 我們先分4群 看群跟群之間的資料
  主要是哪些tags組成



每群的資料數量:

WIFI#9 cluster	WIFI#10 cluster	Null cluster	CRASH#7 cluster
36	36	9	21

常出現的tags

tag	wifi3-1 比例	total RE 出現比例	意義
AIMESH#2	0.56862	0.14856	頻繁啟動cfgsync
CRASH#7	0.50980	0.17163	LOG中出現PC is at ...關鍵字
WIFI#9	0.41176	0.29881	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示2G對上沒有連線
WIFI#10	0.40196	0.4085	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示5GHz-1對上沒有連線
REBOOT#3	0.19607	0.10073	每天都需要定時重開機的使用者。

1. 濾掉 trival case 後主要跟 AIMESH#2、CRASH#7、WIFI#9相關
2. 這三個tags的比例比在RE整體比例高許多

WIFI#9 和 CRASH#7 關係

當發生WIFI#9時會有很高比例發生CRASH#7，反之並沒有很明顯

WIFI#9 cluster:

tag	cluster 內出現比例	total 比例
WIFI#9	1	0.41176
CRASH#7	0.80555	0.50980

CRASH#7 cluster:

tag	cluster 內出現比例	total 比例
CRASH#7	0.8095	0.509803
WIFI#9	0.1045	0.41176

AIMESH#2 在每群的比例都很高

AIMESH#2 total 比例是0.56862

AIMESH#2 在每個cluster的比例:

CRASH#7 cluster:	WIFI#10 cluster:	WIFI#9 cluster:
0.76190	0.38888	0.77777

觀察總結

1. 濾掉 trival case 後主要跟 AIMESH#2、CRASH#7、WIFI#9相關

1. 這三個tags的比例比在RE整體比例高許多

1. 可以觀察到當發生WIFI#9時會有很高比例發生CRASH#7，反之並沒有很明顯

1. AIMESH#2 在每群的比例都很高

1. 不確定WIFI#3-1是不是只有發生在RE上

WIFI#9 cluster:

tag	cluster 內出現比例	total 比例	意義
WIFI#9	1	0.41176	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示2G對上沒有連線
CRASH#7	0.80555	0.50980	LOG中出現PC is at ...關鍵字
AIMESH#2	0.77777	0.56862	頻繁啟動cfgsync
WIFI#10	0.22222	0.40196	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示5GHz-1對上沒有連線

WIFI#10 cluster:

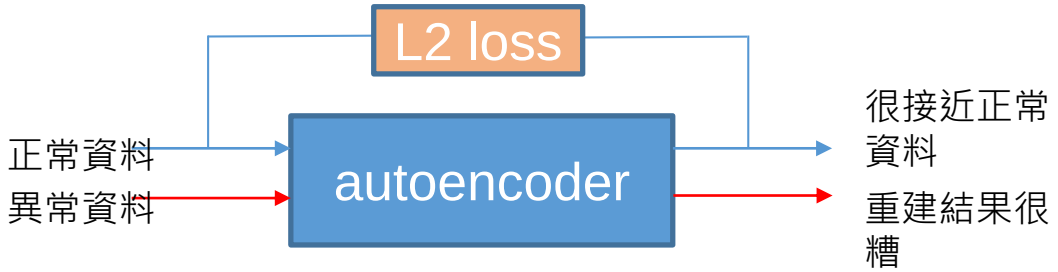
tag	cluster 內出現比例	total 比例	意義
WIFI#10	0.88888	0.40196	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示5GHz-1對上沒有連線
REBOOT#3	0.44444	0.19607	每天都需要定時重開機的使用者。
AIMESH#2	0.38888	0.56862	頻繁啟動cfgsync
WIFI#11	0.30555	0.10784	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示5GHz-2對上沒有連線
CRASH#9	0.22222	0.078431	syslog內容出現crashlog訊息，syslog出現'crashlog:'
CRASH#7	0.16666	0.50980	LOG中出現PC is at ...關鍵字
WIFI#9	0.13888	0.4117	從WlGetDriverStatsXXX.log檔案，檢查是否有[Not associated. Last associated with SSID]表示2G對上沒有連線

CRASH#7 cluster:

tag	cluster 內出現比例	total 比例	意義
CRASH#7	0.8095	0.509803	LOG中出現PC is at ...關鍵字
AIMESH#2	0.76190	0.568627	頻繁啟動cfgsync
ACSD#1	0.1904	0.058823	ACSD update 失敗，造成5GHz 選擇20MHz。

PART III. 異常偵測

非監督式異常偵測



核心概念:異常資料相較於正常資料極少

1. 利用gensim套件中的 doc2vec 把log轉成vector(256維)
2. 使用CNN(input = (batch=32, window=8, 256))來做autoencoder
3. 算(input-output)的Euclidean norm
4. 取mean+3*std當作threshold
5. 超過threshold的window (8行)當作anomaly
6. 觀察anomaly的特性

Anomaly Messages in different firmwares

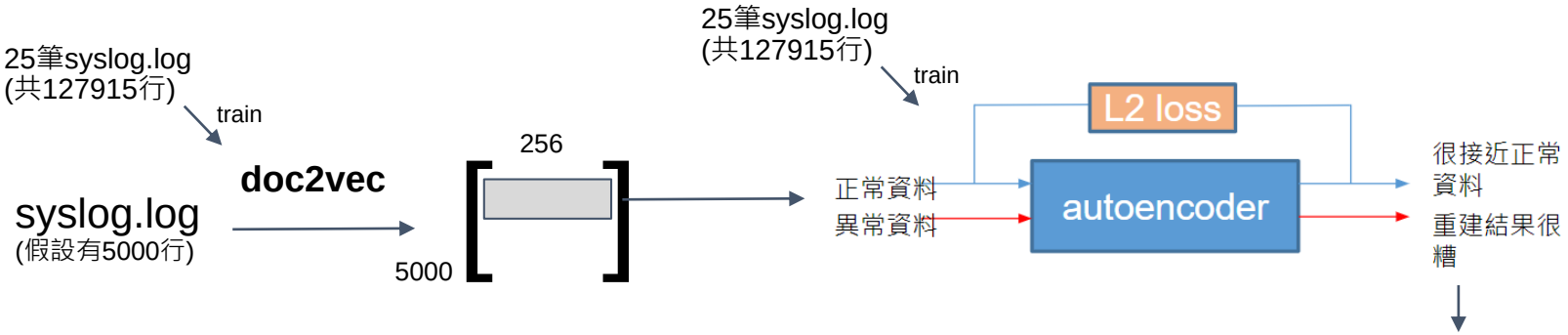
```
================================================================================================
File: doc2vec/RT-AX3000/3.0.0.4.386_41793-gdb31cdc/anomaly.txt
Top-10 Anomaly messages:

wlceventd: wlceventd_proc_event(507): wl1.1: Disassoc 3E:-:-:-:FE:17, status: 0, reason: Disassociated because sending station is leav
ing (or has left) BSS (8), rssi:0
wlceventd: wlceventd_proc_event(526): wl1.1: Auth 3E:-:-:-:FE:17, status: Successful (0), rssi:0
wlceventd: wlceventd_proc_event(507): wl1.1: Disassoc 16:-:-:-:60:F9, status: 0, reason: Disassociated because sending station is leav
ing (or has left) BSS (8), rssi:0
wlceventd: wlceventd_proc_event(555): wl1.1: Assoc 3E:-:-:-:FE:17, status: Successful (0), rssi:0
wlceventd: wlceventd_proc_event(507): wl1.1: Disassoc C6:-:-:-:41:26, status: 0, reason: Disassociated because sending station is leav
ing (or has left) BSS (8), rssi:0
wlceventd: wlceventd_proc_event(526): wl1.1: Auth 16:-:-:-:60:F9, status: Successful (0), rssi:0
wlceventd: wlceventd_proc_event(555): wl1.1: Assoc 16:-:-:-:60:F9, status: Successful (0), rssi:0
wlceventd: wlceventd_proc_event(507): wl1.1: Disassoc 5E:-:-:-:4A:B3, status: 0, reason: Disassociated because sending station is leav
ing (or has left) BSS (8), rssi:0
disk_monitor: Got SIGALRM...
BHC: Topology change from 1 to 0.
================================================================================================
```

To know the ground truth, we need the code for labeling.

異常偵測 (WIFI#3-1)

以25筆 WIFI#3-1全部的 syslog.log train doc2vec,
再以25筆 WIFI#3-1全部的 syslog.log 去 train一個 autoencoder.
最後用每筆資料各自做anomaly detection，觀察抓出來異常的log。




```
Anomaly Messages
wlceventd: wlceventd_proc_event(527): wl2.1: Auth F0:-:-:-:57:A5, status: Successful (0), rssi:-25
wlceventd: wlceventd_proc_event(556): wl2.1: Assoc F0:-:-:-:57:A5, status: Successful (0), rssi:-25
kernel: eth1 (Ext switch port: 0) (Logical Port: 8) (phyId: 0) Link DOWN.
kernel: eth1: sysport_tm port shaper set to 99900 kbps (phy speed 100000 kbps)
kernel: eth1 (Ext switch port: 0) (Logical Port: 8) (phyId: 0) Link Up at 100 mbps full duplex
kernel: eth1 (Ext switch port: 0) (Logical Port: 8) (phyId: 0) Link DOWN.
wlceventd: wlceventd_proc_event(491): wl2.1: Deauth_ind F0:-:-:-:57:A5, status: 0, reason: Deauthenti
wlceventd: wlceventd_proc_event(491): wl2.1: Deauth_ind F0:-:-:-:57:A5, status: 0, reason: Deauthenti
```

異常偵測 (WIFI#3-1) 結果統計

	Anomaly Messages	number of detection	percentage of all dectections
0	kernel: kek:	870	6.97%
1	kernel: replay_ctr:	749	6.00%
2	kernel: kck:	740	5.93%
3	kernel: 0000: 00 00 00 00 00 00 00 02	472	3.78%
4	BHC: WiFi connection status change.	413	3.31%
5	BHC: bandindex(1): state is 0	281	2.25%
6	BHC: bandindex(0): state is 2	214	1.71%
7	BHC: bandindex(2): state is 0	144	1.15%
8	BHC: Topology change from 8 to 2.	116	0.93%
9	kernel: eth1 (Ext switch port: 0) (Logical Port: 8) (phyId: 0) Link DOWN.	105	0.84%
10	BHC: bandindex(0): state is 0	102	0.82%
11	kernel: CSIMON: M2M usr already registered ...	93	0.74%
12	kernel: CSIMON: CSIMON[1.1.0] Initialization	85	0.68%
13	BHC: bandindex(2): state is 2	74	0.59%
14	kernel: eth1: sysport_tm port shaper set to 999000 kbps (phy speed 1000000 kbps)	58	0.46%
15	BHC: Topology change from -1 to 8.	55	0.44%
16	kernel: eth1 (Ext switch port: 0) (Logical Port: 8) (phyId: 0) Link Up at 1000 mbps full duplex	54	0.43%
17	BHC: IN_BR	51	0.41%
18	roamast: ROAMING Start...	47	0.38%
19	kernel: eth1 (Ext switch port: 0) (Logical Port: 8) (phyId: 0) Link Up at 100 mbps full duplex	47	0.38%
20	kernel: eth1: sysport_tm port shaper set to 99900 kbps (phy speed 100000 kbps)	44	0.35%

從結果中可以發現有 Topology change被偵測出來(編號8)。

不過有許多變數(編號3)，可能因為長度長、出現次數少而被當作異常偵測出來。

Parser

將每行的log變成template的形式(捨棄變數)

文獻中用來減少變數帶來的異質性。

Parser會按照我們事先定義的變數和它自己判斷應該是變數的位置來產生template。

事先定義的變數如下:

E2:-:-:-:BB:8C	=> MAC
ffffffc02d590000	=> BASEADDR
0x2d500000	=> PHYSADDR
78 60 69 96 ….	=> ADDR
v1.24.1	=> VERSION
2021-01-08 ….	=> DATETIME
^[[0;34m	=> NOISE

```
rx_post_flow_ring_base_addr : ffffffc02d590000
tx_post_flow_ring_base_addr : ffffffc0092d8000
rx_complete_flow_ring_base_addr : ffffffc02d594000
tx_complete_flow_ring_base_addr : ffffffc02d592000
r2d_wr_arr_base_addr : ffffff8002642000
d2r_rd_arr_base_addr : ffffff8002642802
r2d_rd_arr_base_addr : ffffff8002643000
d2r_wr_arr_base_addr : ffffff8002642c02
tx_post_mgmt_arr_base_addr : ffffff8002643800
tx_post_mgmt_arr_base_phys_addr : 0x2d501800
r2d_wr_arr_base_phys_addr : 0x2d500000
d2r_rd_arr_base_phys_addr : 0x2d500802
r2d_rd_arr_base_phys_addr : 0x2d501000
d2r_wr_arr_base_phys_addr : 0x2d500c02
```

```
May  5 05:06:02 kernel: kck:
May  5 05:06:02 kernel:   0000: 78 60 69 96 08 d0 d7 a6 4a 76 ee d6 3e f6 02 ba
May  5 05:06:02 kernel: kek:
May  5 05:06:02 kernel:   0000: 13 13 d6 f8 95 2f a6 59 0b 81 69 92 35 f4 96 e1
May  5 05:06:02 kernel: replay_ctr:
May  5 05:06:02 kernel:   0000: 00 00 00 00 00 00 00 02
May  5 05:06:03 kernel: kck:
May  5 05:06:03 kernel:   0000: 02 1d 22 6f ff 15 d1 a5 db c2 2a 51 b8 8d 3c 1b
May  5 05:06:03 kernel: kek:
May  5 05:06:03 kernel:   0000: 27 63 57 38 0c 18 79 f6 a7 b7 c4 39 5f 32 4d a7
```

```
 kernel: klogd started: BusyBox v1.24.1 (2021-01-08 18:34:22 CST)
```

```
May  5 05:05:13 kernel: ^[[0;34m[NTC bitpool] idx_pool_init: 551:PktRnr[0]:Create Index
Pool_Size = 16512^[[0m
May  5 05:05:13 kernel: ^[[0;34m[NTC bitpool] idx_pool_init: 551:L2L3-ucast:Create Index
Pool_Size = 16384^[[0m
```

Parser example

```
57  Mar 31 11:41:41 BHC: bandindex(0): state is 2
58  Mar 31 11:41:41 BHC: bandindex(1): state is 2
59  Mar 31 11:41:43 BHC: Topology change from 2 to 4.
60  Mar 31 11:41:51 BHC: WiFi connection status change.
61  Mar 31 11:41:51 BHC: bandindex(0): state is 0
62  Mar 31 11:41:51 BHC: bandindex(1): state is 2
63  Mar 31 11:41:55 BHC: WiFi connection status change.
64  Mar 31 11:41:55 BHC: bandindex(0): state is 2
65  Mar 31 11:41:55 BHC: bandindex(1): state is 2
66  Mar 31 11:47:59 wlceventd: wlceventd_proc_event(527): wl1.1: Auth 6A:-:-:-:70:92, status: Successful (0), rssi:0
67  Mar 31 11:47:59 wlceventd: wlceventd_proc_event(537): wl1.1: ReAssoc 6A:-:-:-:70:92, status: Successful (0), rssi:-84
68  Mar 31 11:48:14 roamast: determine candidate node [24:-:-:-:60:AC](rssi: -35dbm) for client [6A:-:-:-:70:92](rssi: -74dbm) to roam
69  Mar 31 11:48:14 roamast: Roam a client [6A:-:-:-:70:92], status [0]
70  Mar 31 11:48:18 roamast: [EXAP]Deauth old sta in 1 1: 6A:-:-:-:70:92
71  Mar 31 11:48:18 roamast: wl1.1: disconnect weak signal strength station [6a:-:-:-:70:92]
72  Mar 31 11:48:18 roamast: wl1.1: remove client [6a:-:-:-:70:92] from monitor list
73  Mar 31 11:48:18 wlceventd: wlceventd_proc_event(491): wl1.1: Deauth_ind 6A:-:-:-:70:92, status: 0, reason: Deauthenticated because sending station is leaving (or has left) IBSS or ESS (3), rssi:-87
74  Mar 31 11:48:18 wlceventd: wlceventd_proc_event(491): wl1.1: Deauth_ind 6A:-:-:-:70:92, status: 0, reason: Deauthenticated because sending station is leaving (or has left) IBSS or ESS (3), rssi:-87
```

```
57  Mar 31 11:41:41 BHC: bandindex(<:NUM:>): state is <:*:>
58  Mar 31 11:41:41 BHC: bandindex(<:NUM:>): state is <:*:>
59  Mar 31 11:41:43 BHC: Topology change from <:NUM:> to <:NUM:>.
60  Mar 31 11:41:51 BHC: WiFi connection status <:*:>
61  Mar 31 11:41:51 BHC: bandindex(<:NUM:>): state is <:*:>
62  Mar 31 11:41:51 BHC: bandindex(<:NUM:>): state is <:*:>
63  Mar 31 11:41:55 BHC: WiFi connection status <:*:>
64  Mar 31 11:41:55 BHC: bandindex(<:NUM:>): state is <:*:>
65  Mar 31 11:41:55 BHC: bandindex(<:NUM:>): state is <:*:>
66  Mar 31 11:47:59 wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Auth <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>
67  Mar 31 11:47:59 wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> ReAssoc <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>
68  Mar 31 11:48:14 roamast: determine candidate node [<:MAC:>](rssi: <:*:> for client [<:MAC:>](rssi: <:*:> to roam
69  Mar 31 11:48:14 roamast: Roam a client [<:MAC:>], status [<:NUM:>]
70  Mar 31 11:48:18 roamast: [EXAP]Deauth old sta in <:NUM:> <:NUM:>: <:MAC:>
71  Mar 31 11:48:18 roamast: <:*:> disconnect weak signal strength station <:*:>
72  Mar 31 11:48:18 roamast: <:*:> remove client <:*:> from monitor list
73  Mar 31 11:48:18 wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Deauth_ind <:MAC:>, status: <:NUM:>, reason: Deauthenticated because sending station is leaving (or has left) IBSS or ESS (<:NUM:>), rssi:<:NUM:>
74  Mar 31 11:48:18 wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Deauth_ind <:MAC:>, status: <:NUM:>, reason: Deauthenticated because sending station is leaving (or has left) IBSS or ESS (<:NUM:>), rssi:<:NUM:>
```

加上parser後的異常偵測 (WIFI#3-1) 結果統計

	Anomaly Messages	number of detection	
0	wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Deauth_ind <:MAC:>, status: <:NUM:>, reason: Deauthenticated because sending station is leaving (or has left) IBSS or ESS (<:NUM:>), rssi:<:NUM:>	868	9.78%
1	wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Disassoc <:MAC:>, status: <:NUM:>, reason: <:*:> <:*:> <:*:> <:*:> <:*:> <:*:> <:*:> <:*:> <:*:> <:*:> <:*:> (<:NUM:>), rssi:<:NUM:>	501	5.65%
2	syslog: wlceventd_proc_event(<:NUM:>): <:*:> Deauth_ind <:MAC:>, status: <:NUM:>, reason: Deauthenticated because sending station is leaving (or has left) IBSS or ESS (<:NUM:>), rssi:<:NUM:>	255	2.87%
3	wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Auth <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>	239	2.69%
4	syslog: wlceventd_proc_event(<:NUM:>): <:*:> Auth <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>	212	2.39%
5	kernel: <:*:>	193	2.18%
6	roamast: <:*:> remove client <:*:> from monitor list	139	1.57%
7	wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> Assoc <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>	139	1.57%
8	syslog: wlceventd_proc_event(<:NUM:>): <:*:> Assoc <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>	126	1.42%
9	BHC: bandindex(<:NUM:>): state is <:*:>	126	1.42%
10	roamast: <:*:> disconnect weak signal strength station <:*:>	123	1.39%
11	syslog: wlceventd_proc_event(<:NUM:>): <:*:> Disassoc <:MAC:>, status: <:NUM:>, reason: Disassociated because sending station is leaving (or has left) BSS (<:NUM:>), rssi:<:NUM:>	122	1.38%
12	kernel: <:NUM:>: <:*:> <:*:>	120	1.35%
13	wlceventd: wlceventd_proc_event(<:NUM:>): <:*:> ReAssoc <:MAC:>, status: Successful (<:NUM:>), rssi:<:NUM:>	119	1.34%
14	kernel: CONSOLE: <:NUM:>.<:NUM:> <:*:> wlc_send_bar: for <:*:> seq <:HEX:> tid <:NUM:>	108	1.22%
15	kernel: <:*:> (Ext switch port: <:NUM:>) (Logical Port: <:NUM:>) (phyId: <:*:> Link DOWN.	102	1.15%
16	kernel: <:*:> (Ext switch port: <:NUM:>) (Logical Port: <:NUM:>) (phyId: <:*:> Link <:*:> at <:NUM:> mbps <:*:> duplex	97	1.09%
17	roamast: [EXAP]Deauth old sta in <:NUM:> <:NUM:>: <:MAC:>	92	1.04%
18	kernel: <:*:> sysport_tm port shaper set to <:*:> kbps (phy speed <:*:> kbps)	91	1.03%
19	kernel: creating mapping for reserved memory phys <:PHYSADDR2:> virt <:BASEADDR2:> size <:PHYSADDR2:> for <:*:>	87	0.98%
20	kernel: <:*:> <:*:> is <:*:>	82	0.92%

加上parser後的異常偵測中統計結果，前幾名都是wlceventd(編號0,1,2,3,4,7,8,11,13)

請問這和WIFI#3-1有沒有相關性?

有沒有辦法從這些的異常偵測結果，推論這些資料屬於WIFI#3-1類型的問題?

後續

- 根據今天的討論，修改異常偵測的Model，對WIFI#3-1這類的資料做更深入的診斷。