Some things about LAN device detection
(關於內網設備識別的二三事)

Canaan Kao, Terence Liu, Hsien-Wei Hung and Ryan Lung
canaan_kao@trend.com.tw

Network Threat Defense Technology Group
Trend Micro

Who we are

- Network Threat Defense Technology Group (NTDTG) of Trend Micro
  - We have offices in Hsinchu and Taipei.
- We focus on
  - (Virtualized) High-speed IPS/IDS
  - Network-stream-based AV
  - Smart-home Protection
  - IoT Security

Before we start

- HitCon2014 slogan:
  - Adapt to the new era of security threats
  - 威脅是一定會有的，我們要學會適應。
- HitCon2015 slogan:
  - Security of Things
  - 物連網安全。
- The combination:
  - Adapt to the new era of IoT security threats.
  - 物連網威脅是一定會有的，我們要學會適應。

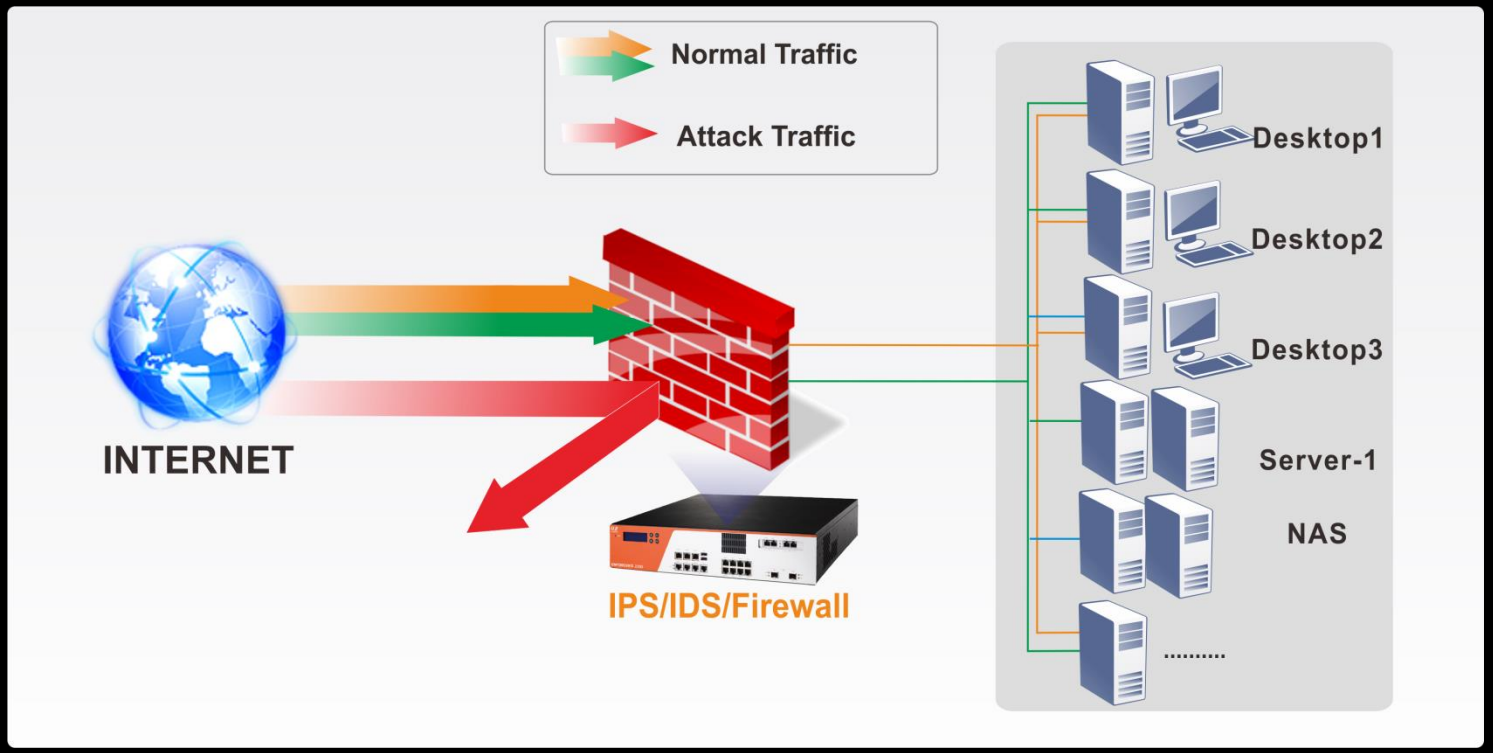
Agenda

- Why LAN device identification (LDI)
- How to detect LAN devices
- The threat intelligence with LDI
- Summary

- Why LAN device identification

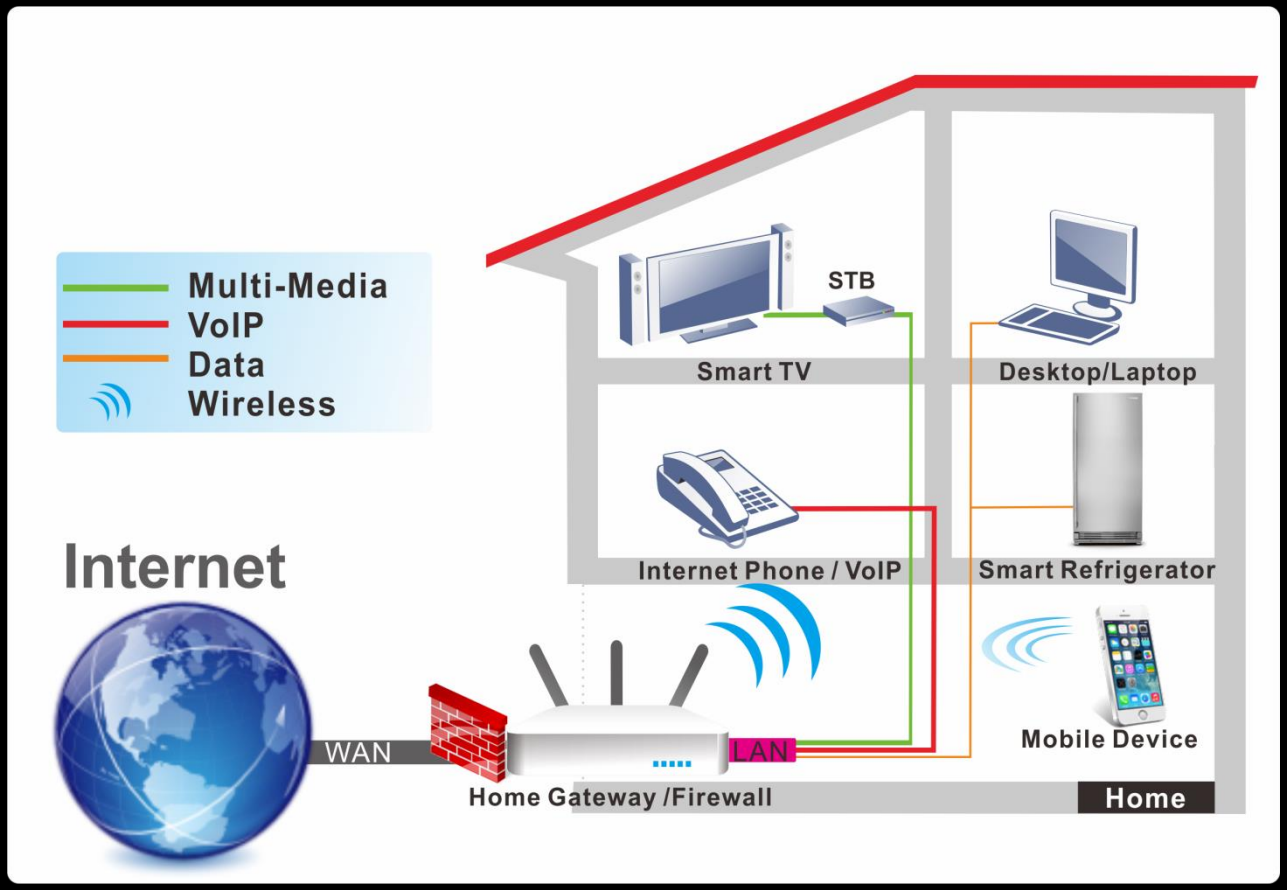
Why LAN device identification

- 過去FW/IDS/IPS 基本上會以為家裡的設備是這樣？



Why LAN device identification

- 但是，家裡連網的設備實際上可能會是....



Why LAN device identification

- 萬一有誤會，就會產生拿針對 x86 產生的特徵碼來偵測攻擊 ARM/MIPS 設備的 shellcode 的狀況….
- ~~User 通常不知道~~

Why LAN device identification

- Monitoring
  - 計量
- Access Control
  - 連網控制
- Learning
  - 知己, LAN device behavior modeling
  - 知彼, Threat intelligence

Why LAN device identification

- Device identification is not important for traditional IDS/IPS?
  - Age is changed.
  - IDS/IPS need to change too.

Why LAN device identification

- PC 上的 Botnet/Malware 會讓自己看起來越來越正常。例如：透過 Dropbox 通訊、看Blog等等。
  - 這樣比較好規避 AV/IPS/FW.

Why LAN device identification

- 可是其他的智慧家電呢？例如：冰箱。
  - 對 PC 來說是正常的行為，對其他的 devices/things 來說，可能還是算異常。

Why LAN device identification

- 所以，問題是，我怎麼知道目前在送 emails 的是台什麼樣的機器？
  - 是 PC? 還是冰箱？哪個牌子? 型號? 病歷？

- How to detect LAN devices

How to detect LAN devices

- 基本上，方法有兩種
  - 1. 主動進行 device fingerprinting scan
    - 就像是 Nmap 的 OS fingerprinting
    - 缺點是容易被發現，且增加不必要的 traffic
  - 2. 被動觀察 devices 送出來的 packets
    - 優點是隱密性高
    - 缺點是相關的 packets 一定要流經過
    - (我們用這種)

How to detect LAN devices

- 被動式的 LAN Device Identification 可以怎麼做？
  - 0. Are you router/NAT or devices?
  - 1. Check the OUI of MAC address
  - 2. Check the DHCP options
  - 3. Check the user-agent of HTTP request
  - 4. Check the used applications
    - 例如：發現它常用 Skype ，那就猜它應該是 PC/phone?
  - 5. Check 其他…
    - 習慣用的 DNS 與 互連的 IP 等等
  - 綜合這些 features, 我們就可以來 算分數/learn ☺

How to detect LAN devices NAT/Router detection

- 如果某個IP是台 router/NAT，而我們在它的 WAN 端
  - 所轄設備的 MAC addresses，我們應該看不到
  - 所轄設備的 DHCP packets，我們應該看不到
  - 該 IP 所呈現的 user-agents 與 application traffic 可能會太多樣

How to detect LAN devices NAT/Router detection

- Two keys
  - The ID field in IP Header
    - In general, NAT does not modify IP ID.
    - If an host presents multiple IP ID sequences, it may be a NAT.
  - The TTL field in IP Header
    - If you are in LAN and you find the packet's TTL is not the initial value (128 for Windows), the packet may be NATed or routed.

How to detect LAN devices NAT/Router detection

- 主要我們會觀察 IP header 的兩個欄位

IPv4 Header Format

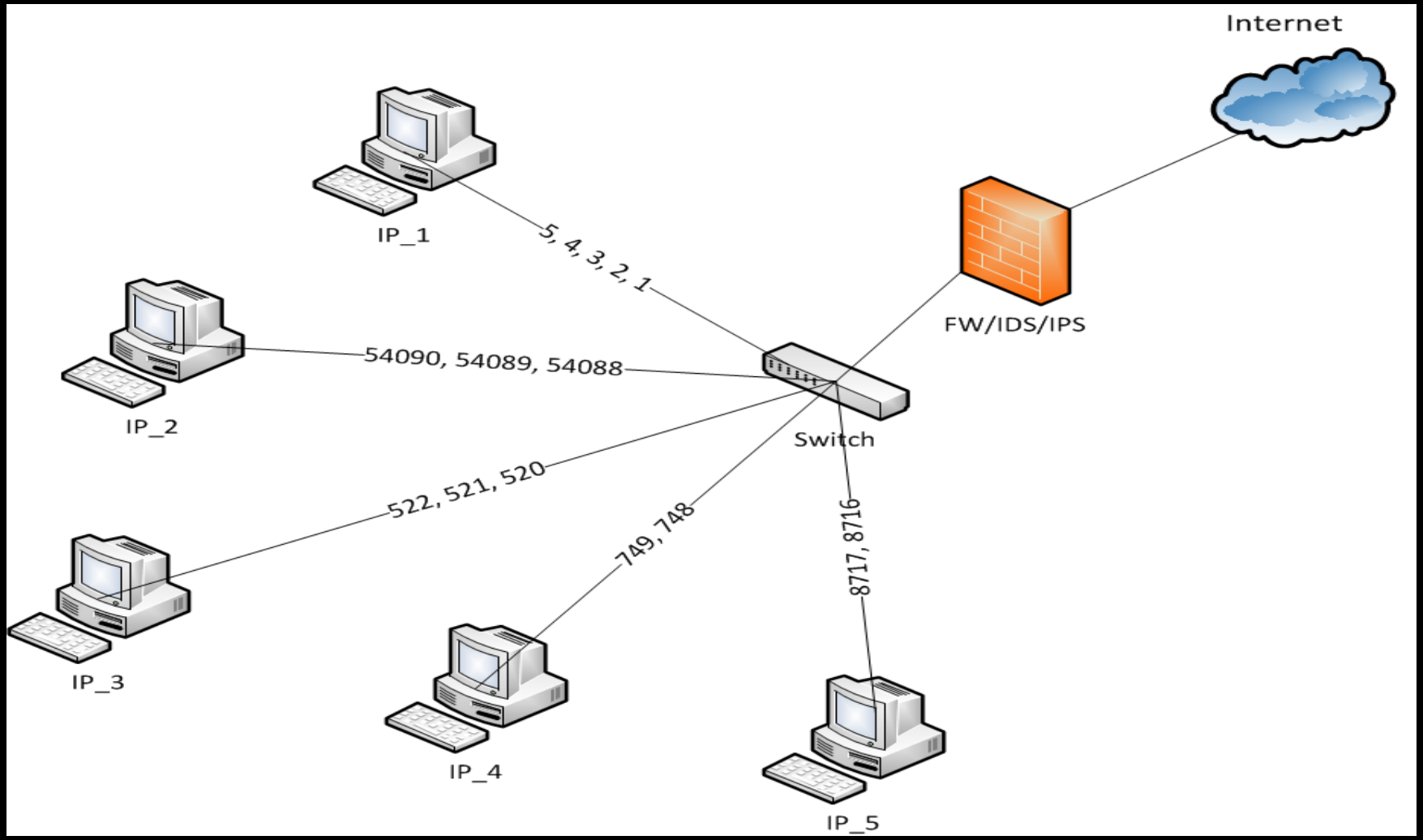
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags				Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

How to detect LAN devices
NAT/Router detection
The ID field in IP Header

- 有些 OS (例如 Win7) 會習慣用同一個 counter 來設定所有送出的 IP ID。
  - 所以，如果一個IP送出來的 packets 其 IP ID 都是以同一個序列遞增，那它應該是台 host。
  - 如果不是，那就要再看其他的。

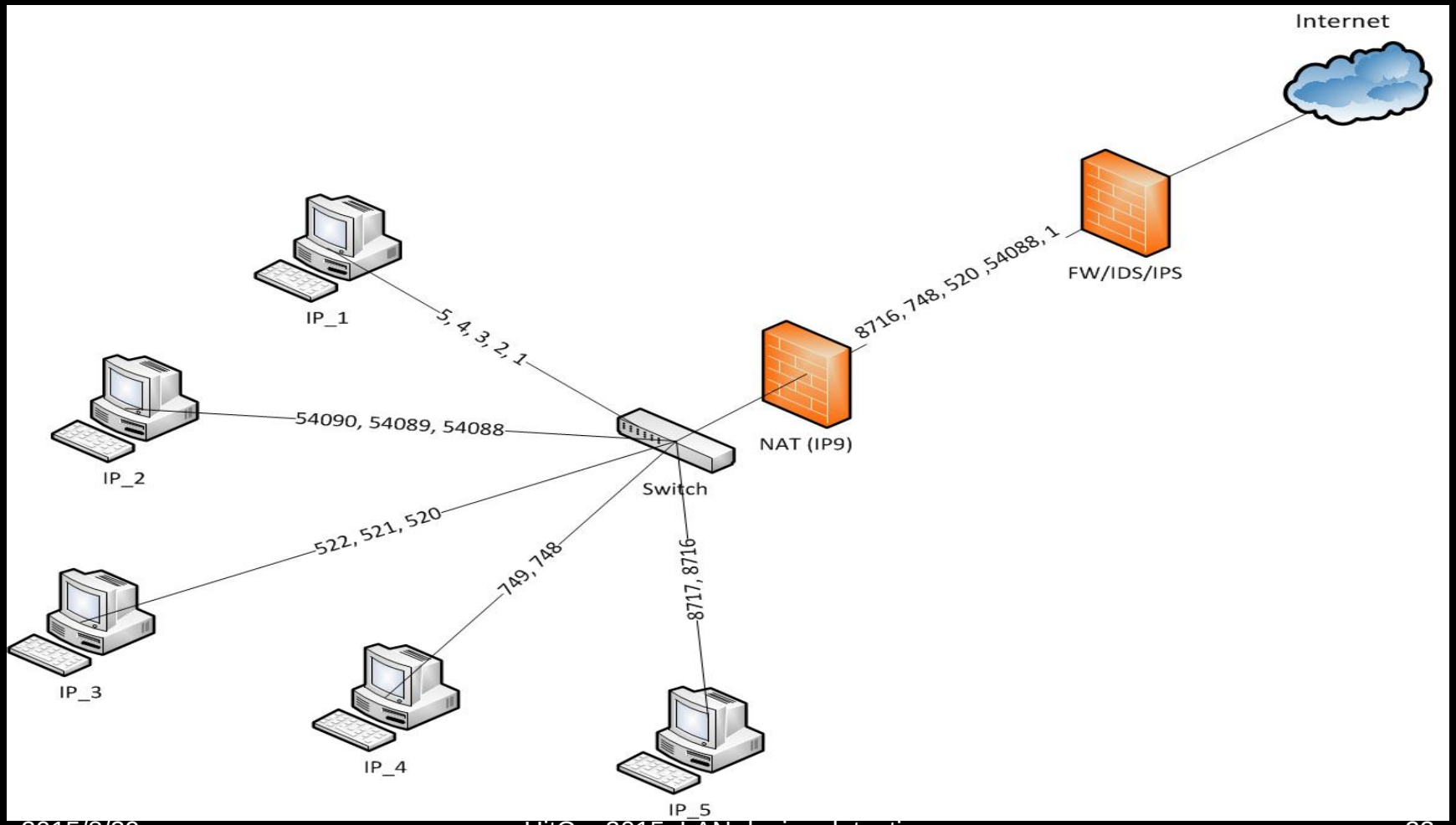
How to detect LAN devices
NAT/Router detection
The ID field in IP Header

- 如果沒有經過 NAT，那我們看到的 IP ID 序列有可能長這樣。



How to detect LAN devices
NAT/Router detection
The ID field in IP Header

- 如果有經過 NAT，那我們看到的 IP ID 序列有可能長這樣。



How to detect LAN devices
NAT/Router detection
The ID field in IP Header

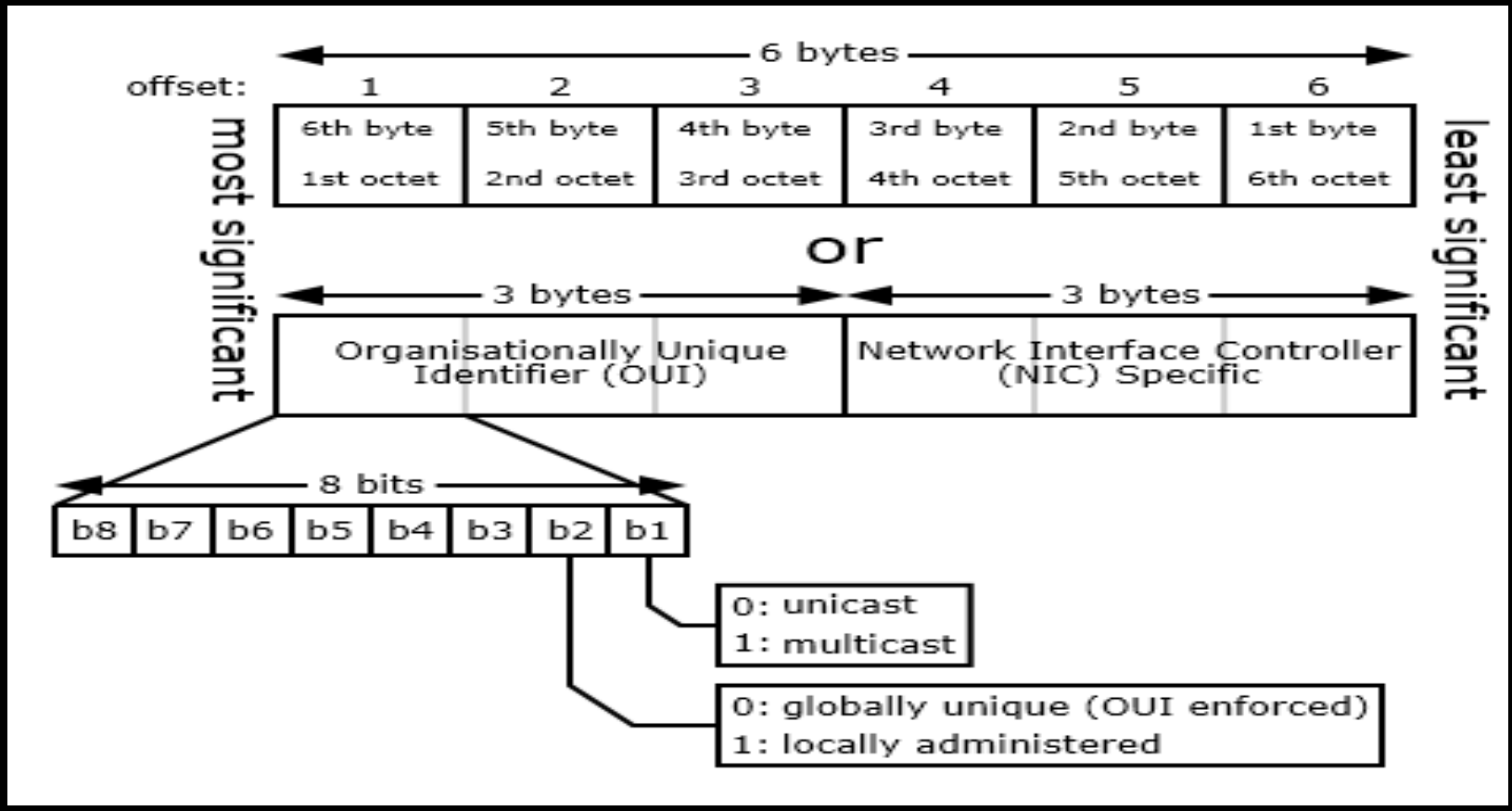
- 所以，如果要偵測家裡的設備，最好的方式就是和 home router 廠商合作。
  - 除非家裡有另外的 NAT，要不然我們就可以免除家裡的困擾。

How to detect LAN devices
NAT/Router detection
The TTL field in IP Header

- TTL 通過 NAT/Router 就會被減一。
  - 所以如果我們看到的封包的 TTL 不是 default value，那它有可能先經過 NAT/Router.
  - Default values:
    - Win7_TCP: 128
    - Ubuntu_TCP: 64

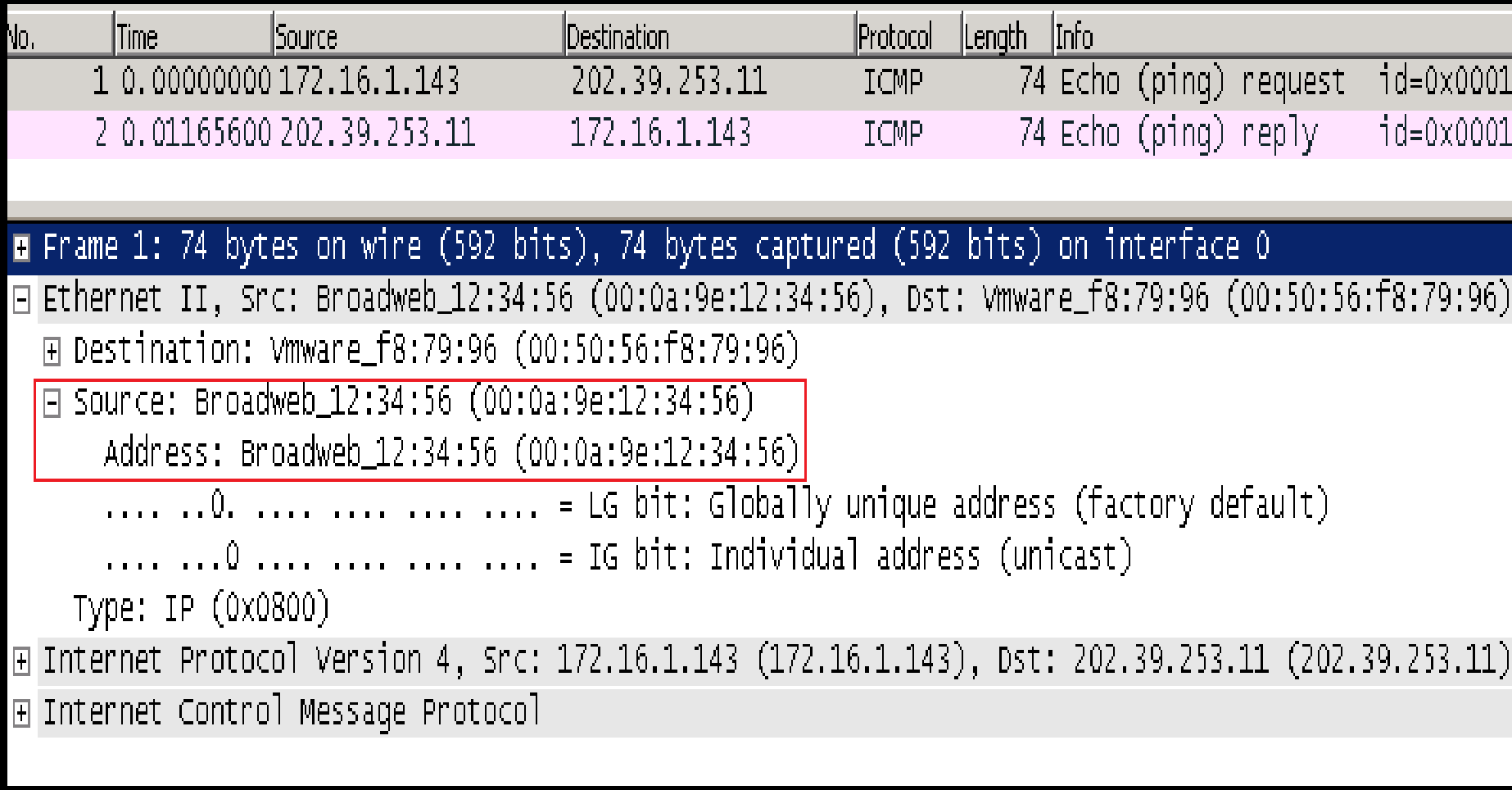
- Ref: http://www.binbert.com/blog/2009/12/default-time-to-live-ttl-values/

How to detect LAN devices
1. Check the OUI of MAC address

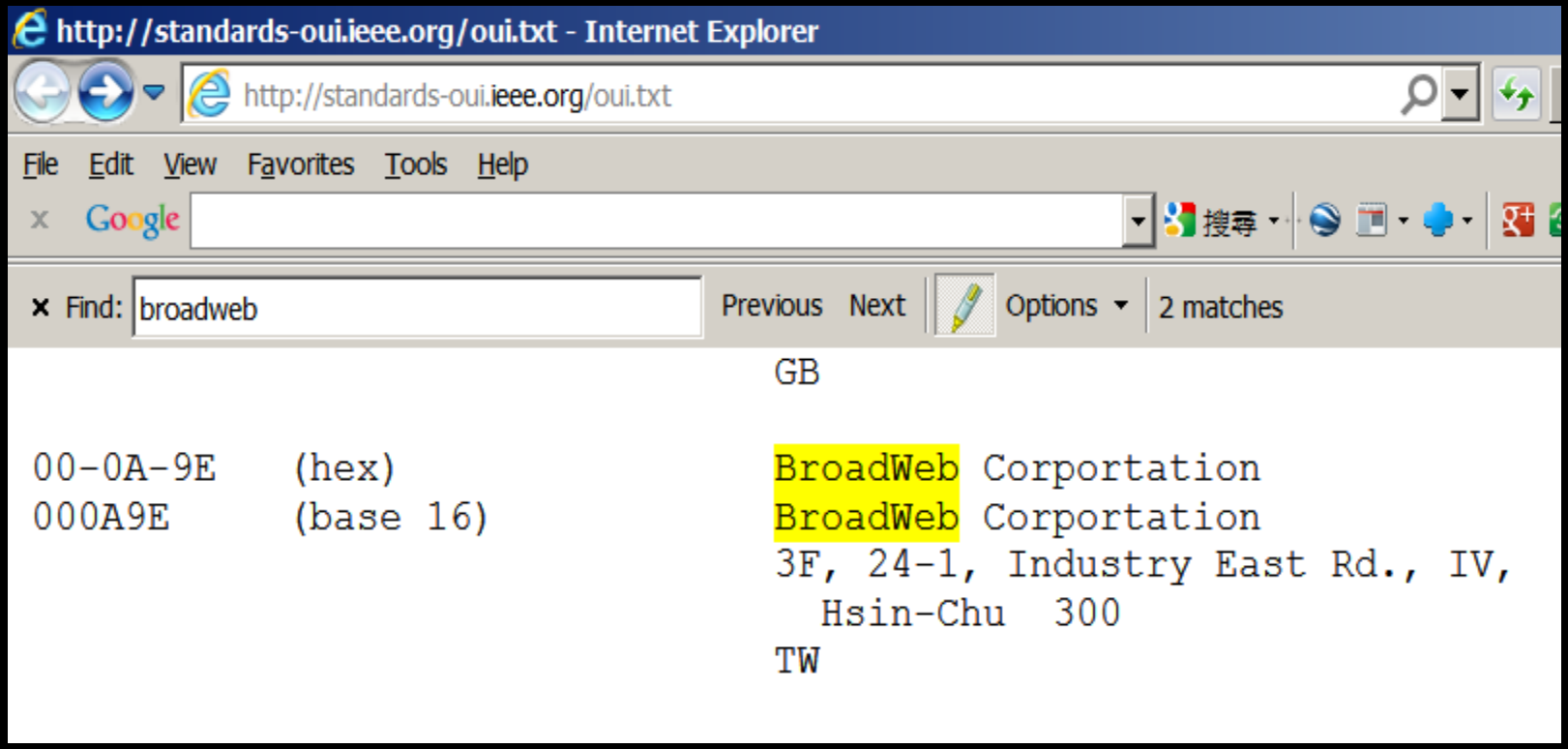


- Source: https://en.wikipedia.org/wiki/MAC_address

How to detect LAN devices
1. Check the OUI of MAC address



How to detect LAN devices
1. Check the OUI of MAC address



- Source: http://standards-oui.ieee.org/oui.txt

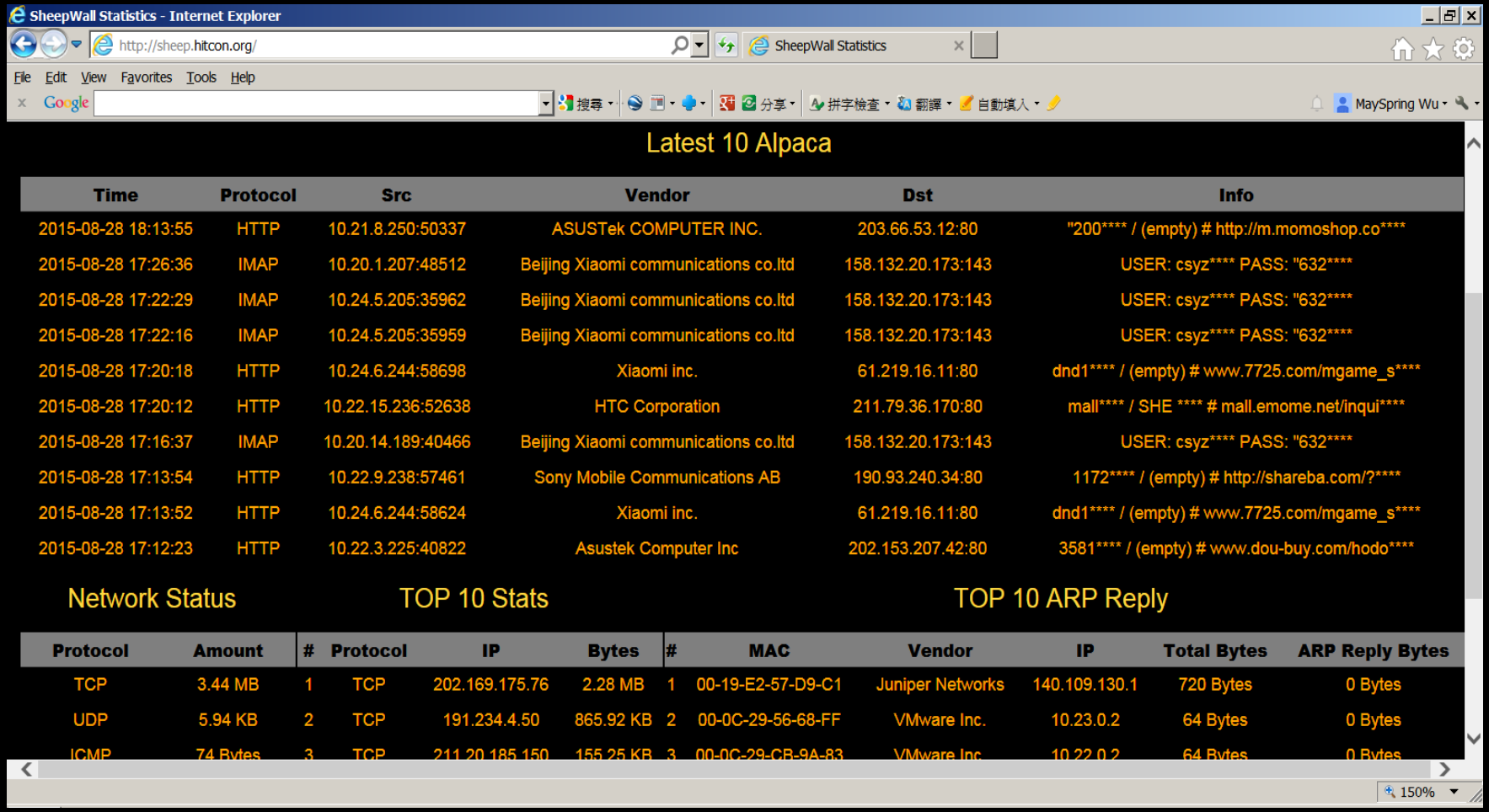
How to detect LAN devices
1. Check the OUI of MAC address

```
$ cat oui.txt | grep -i apple | grep -i "(base 16)" | sort
000393     (base 16)                Apple
000502     (base 16)                Apple
000A27     (base 16)                Apple
000A95     (base 16)                Apple
000D93     (base 16)                Apple
0010FA     (base 16)                Apple
001124     (base 16)                Apple
001451     (base 16)                Apple
0016CB     (base 16)                Apple
0017F2     (base 16)                Apple
0019E3     (base 16)                Apple
001B63     (base 16)                Apple
001CB3     (base 16)                Apple
```

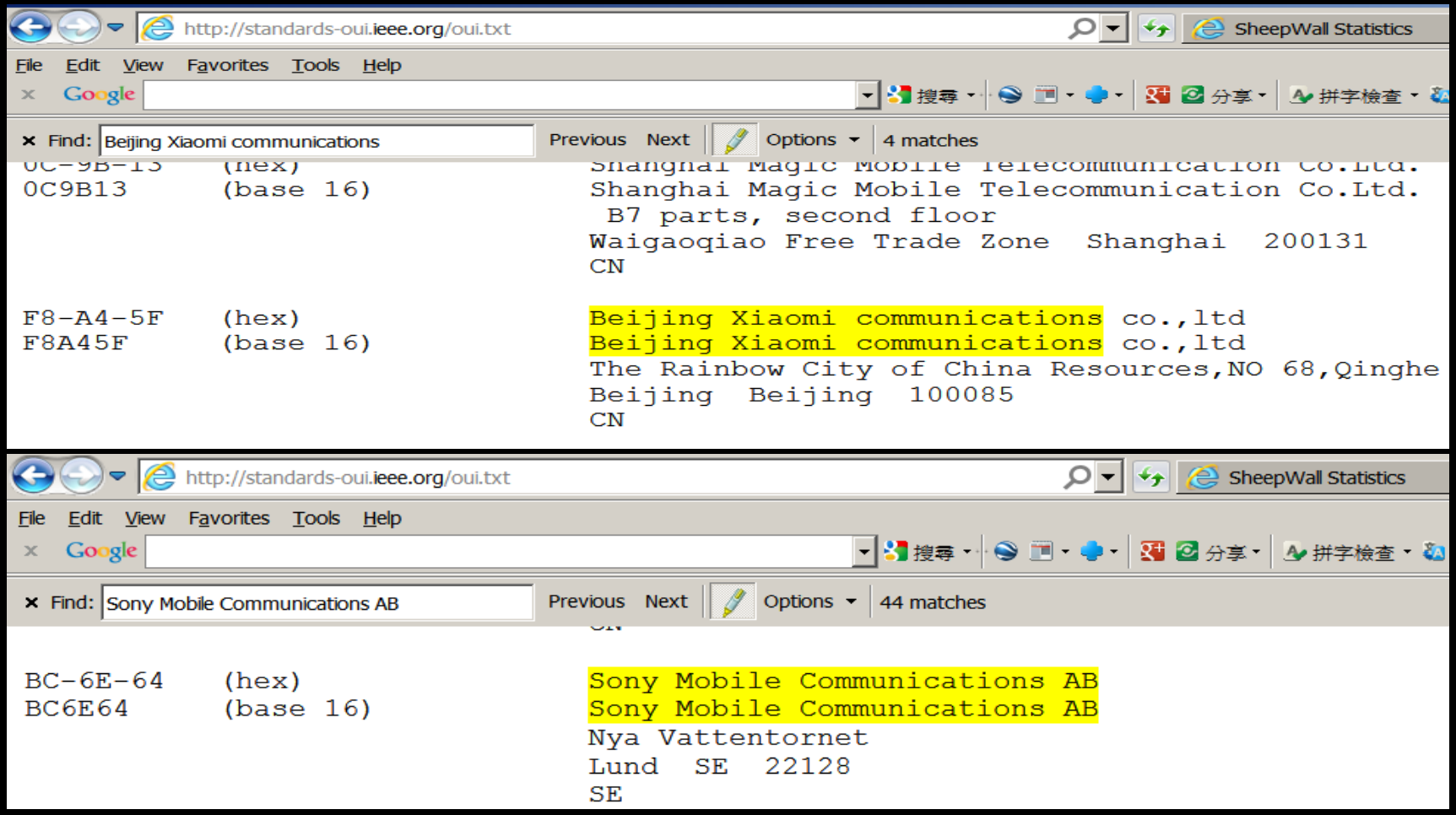
```
$ cat oui.txt | grep -i apple | grep -i "(base 16)" | wc -l
406
```

- 基本上透過 OUI 的檢查，我們可以知道廠牌

How to detect LAN devices
1. Check the OUI of MAC address
應用：綿羊牆



How to detect LAN devices
1. Check the OUI of MAC address
應用：綿羊牆

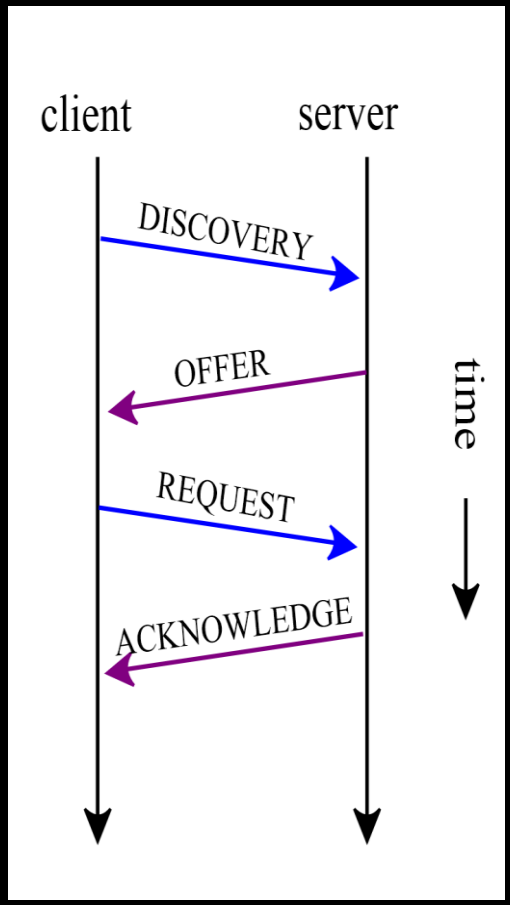


How to detect LAN devices 2. Check the DHCP options

- Why?
  - 有人買 home router/gateway 回家啟用後，沒開 DHCP 的嗎?
    - 有普遍性
  - DHCP Client 有可能洩漏些可識別的資訊給 DHCP Server
  - 以及中間偷聽的設備 ☺

How to detect LAN devices 2. Check the DHCP options

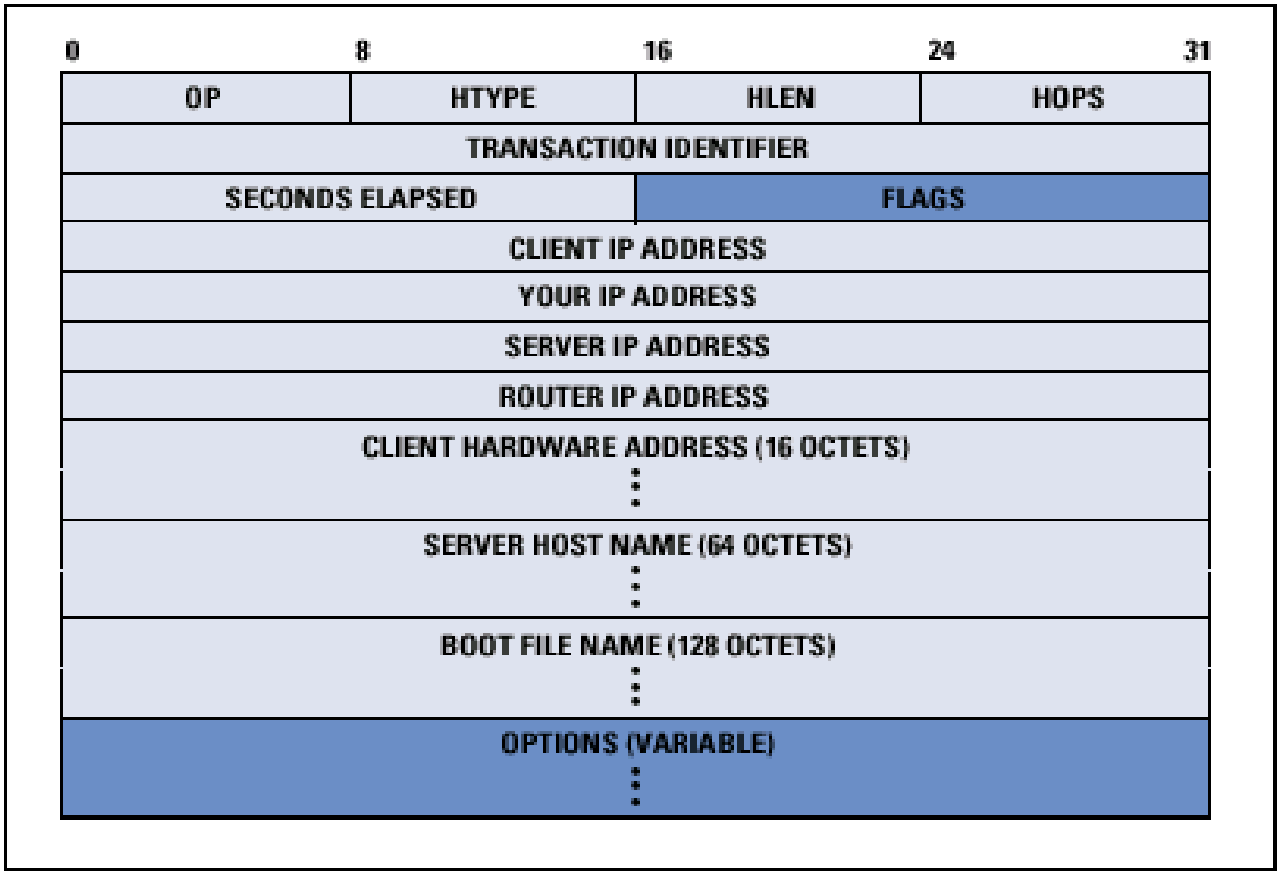
- Dynamic Host Configuration Protocol (DHCP) is based on BOOTP.
  - UDP port 67 for server
  - UDP port 68 for client



- Source: https://upload.wikimedia.org/wikipedia/commons/e/e4/DHCP_session.svg

How to detect LAN devices
2. Check the DHCP options

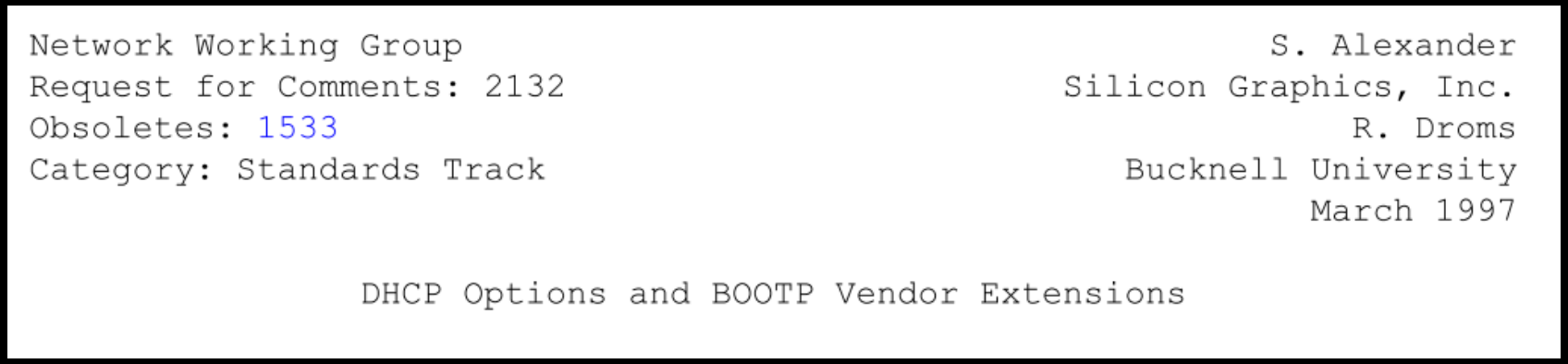
Figure 2: DHCP Message Format



- Source: http://www.cisco.com/web/about/ac123/ac147/images/ipj/ipj_5-2/figure_2_dhcp.gif

How to detect LAN devices
2. Check the DHCP options

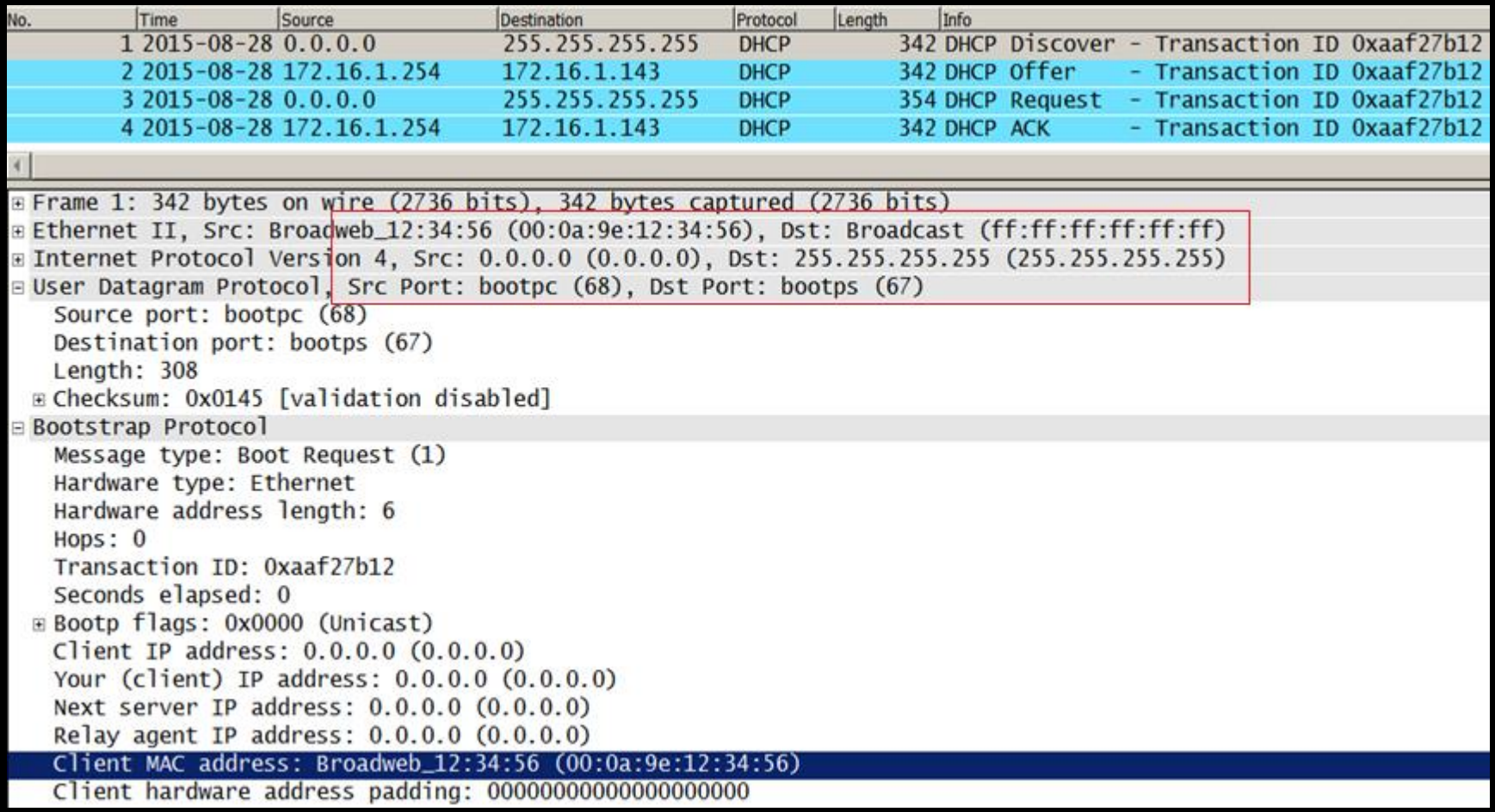
For the details of DHCP options,
please check RFC 2132.



Network Working Group — S. Alexander
Request for Comments: 2132 — Silicon Graphics, Inc.
Obsoletes: 1533 — R. Droms
Category: Standards Track — Bucknell University
March 1997

DHCP Options and BOOTP Vendor Extensions

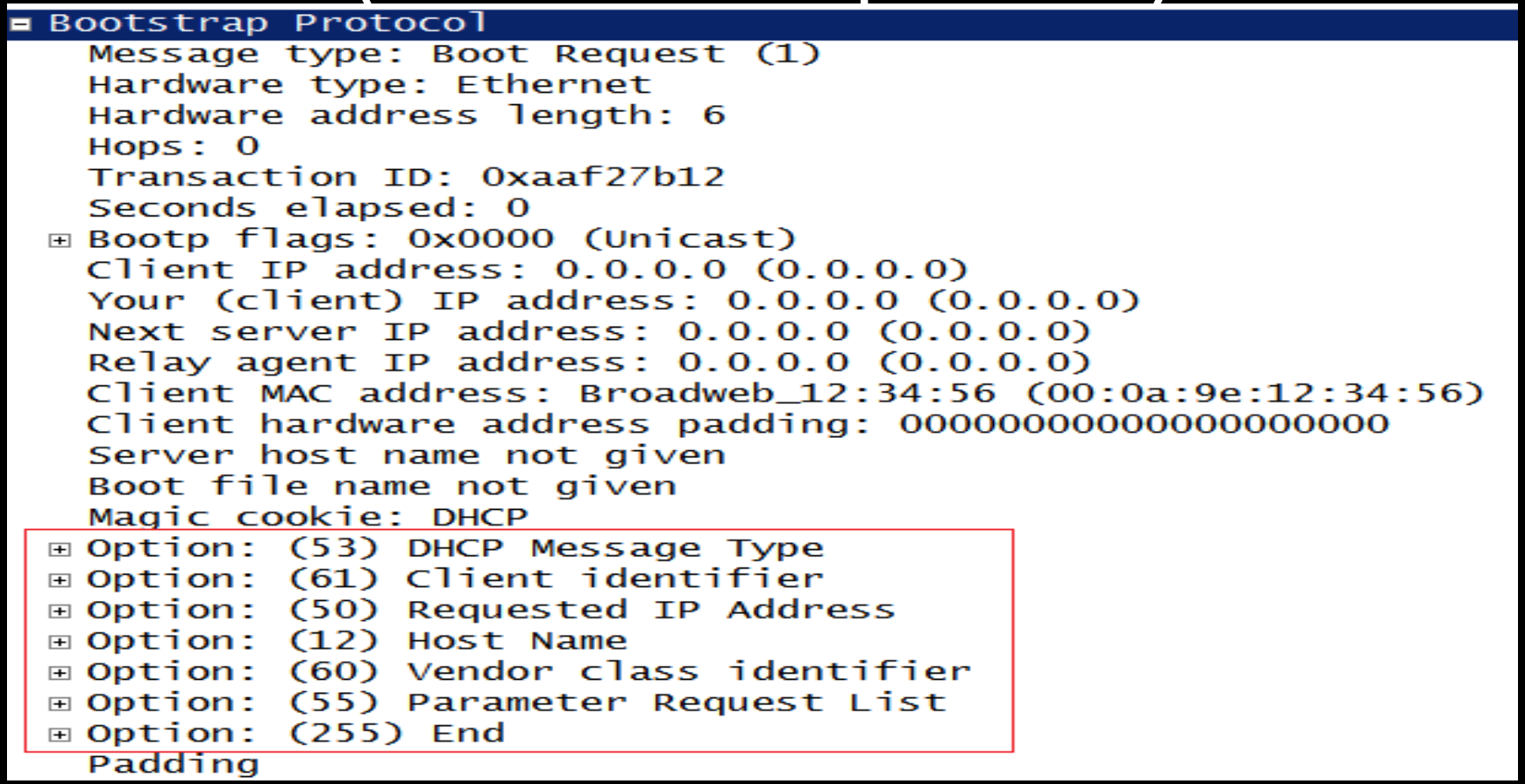
How to detect LAN devices
2. Check the DHCP options



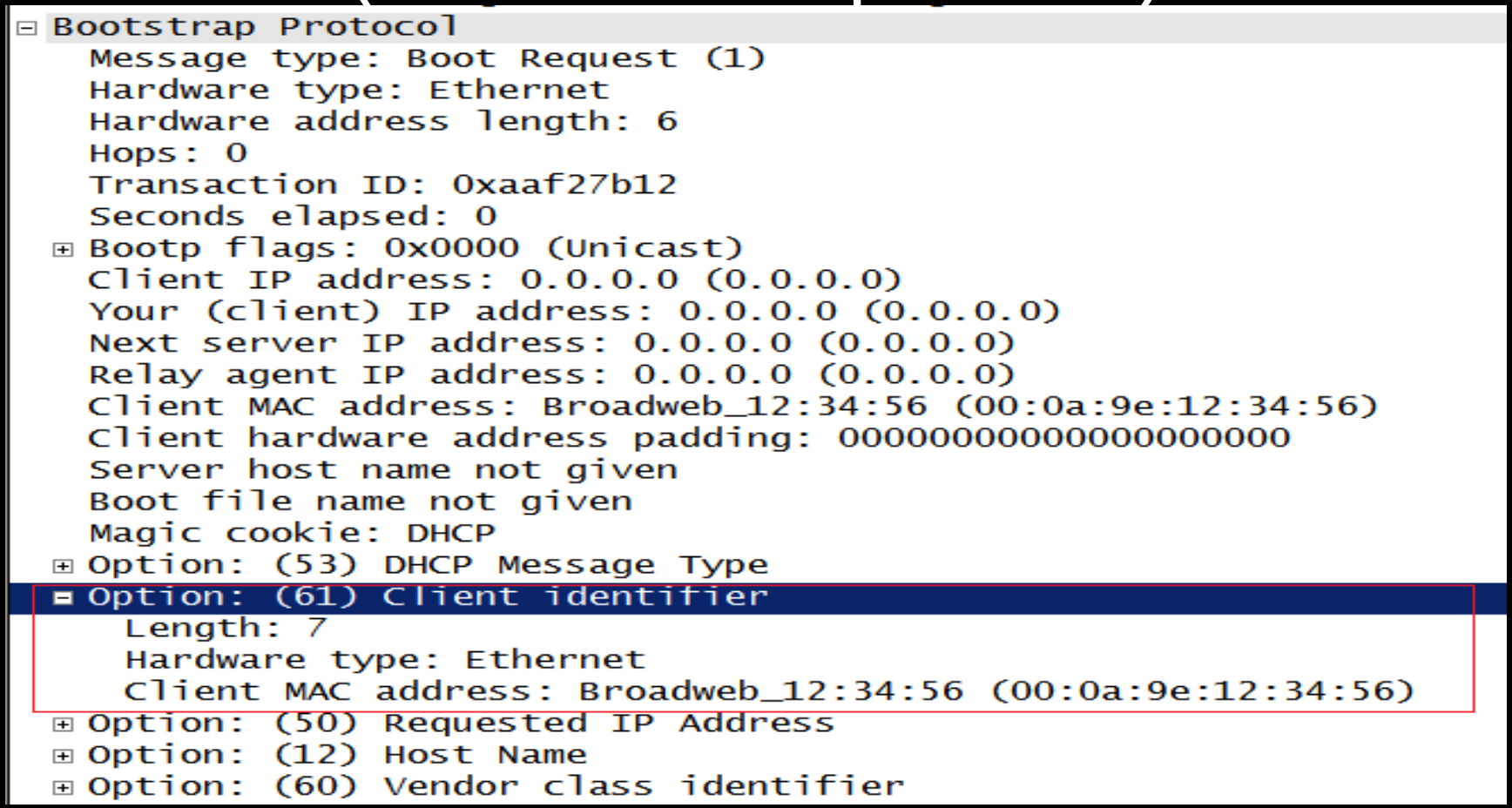
No.	Time	Source	Destination	Protocol	Length	Info
1	2015-08-28	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xaaf27b12
2	2015-08-28	172.16.1.254	172.16.1.143	DHCP	342	DHCP Offer - Transaction ID 0xaaf27b12
3	2015-08-28	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0xaaf27b12
4	2015-08-28	172.16.1.254	172.16.1.143	DHCP	342	DHCP ACK - Transaction ID 0xaaf27b12

```
⊞ Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
⊞ Ethernet II, Src: Broadweb_12:34:56 (00:0a:9e:12:34:56), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊟ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
    Source port: bootpc (68)
    Destination port: bootps (67)
    Length: 308
  ⊞ Checksum: 0x0145 [validation disabled]
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xaaf27b12
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Broadweb_12:34:56 (00:0a:9e:12:34:56)
    Client hardware address padding: 00000000000000000000
```

How to detect LAN devices
2. Check the DHCP options (Win7 DHCP packets)

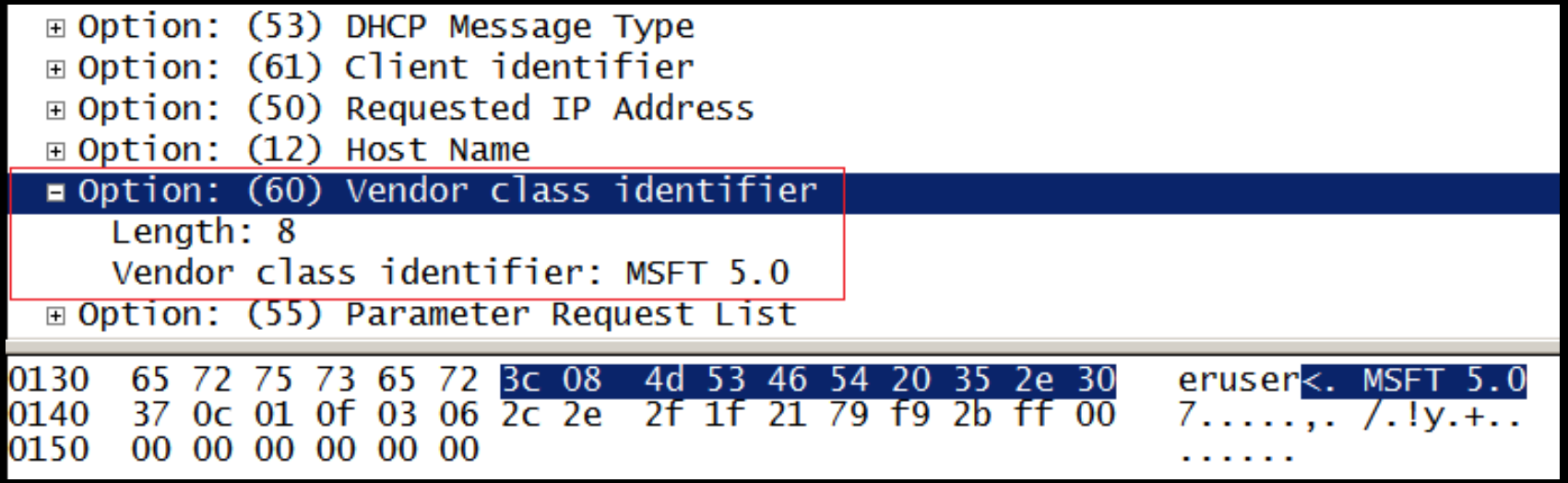


How to detect LAN devices
2. Check the DHCP options
(Win7 DHCP packets)



How to detect LAN devices 2. Check the DHCP options (Win7 DHCP packets)

- 這個 option 有用



How to detect LAN devices
2. Check the DHCP options
(Win7 DHCP packets)

- 這個 option 也有用

```
⊞ Option: (53) DHCP Message Type
⊞ Option: (61) Client identifier
⊞ Option: (50) Requested IP Address
⊞ Option: (12) Host Name
⊞ Option: (60) Vendor class identifier
⊟ Option: (55) Parameter Request List
    Length: 12
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (43) Vendor-Specific Information
⊞ Option: (255) End
  Padding
```

```
0130  65 72 75 73 65 72 3c 08  4d 53 46 54 20 35 2e 30   eruser<. MSFT 5.0
0140  37 0c 01 0f 03 06 2c 2e  2f 1f 21 79 f9 2b ff 00   7.....,. /.!y.+..
0150  00 00 00 00 00 00                                  ......
```

How to detect LAN devices 2. Check the DHCP options

- Option 55/0x37 要怎麼用？
  - 把 request 序列直接當特徵碼
    - 因為 request list 會因為各家 DHCP client 的實作不同而有所不同
  - 以剛剛那個 Win7 packet 為例，
    - 先找到 Option 55/0x37,跳過一個 byte (長度), 再比
    - 0x01, 0x0f, 0x03, 0x06, 0x2c, 0x2e, 0x2f, 0x1f, 0x21, 0x79, 0xf9, 0x2b
    - 1,15,3,6,44,46,47,31,33,121,249,43

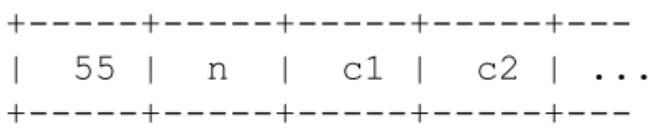
How to detect LAN devices
2. Check the DHCP options

9.8. Parameter Request List

This option is used by a DHCP client to request values for specified configuration parameters. The list of requested parameters is specified as n octets, where each octet is a valid DHCP option code as defined in this document.

The client MAY list the options in order of preference. The DHCP server is not required to return the options in the requested order, but MUST try to insert the requested options in the order requested by the client.

The code for this option is 55. Its minimum length is 1.



How to detect LAN devices 2. Check the DHCP options

- 一些 DHCP option 55 特徵碼 [2][4]
  - For Win7/Server2008
    - 1,15,3,6,44,46,47,31,33,121,249,43
  - For Win 8
    - 1,15,3,6,44,46,47,31,33,121,249,252,43
    - 1,3,6,15,33,44,46,47,121,249,43,60,212
  - For Apple iPod, iPhone or iPad
    - 1,3,6,15,119,78,79,95,252
    - 1,3,6,15,119,252
    - 1,3,6,15,119,252,46,208,92
    - 1,3,6,15,119,252,67,52,13

How to detect LAN devices
3. Check the user-agent of HTTP

- 有時候，檢查 Browser 的 user-agent 裡面的 keywords 也是一個選項。
  - 的確，user-agent 比 MAC address 或是 DHCP option 55 更容易被假造。
  - 沒有辦法時的辦法，加減用一下 ☺

How to detect LAN devices
3. Check the user-agent of HTTP

- IE11 on Win7
  - User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0; GTB7.5) like Gecko
- iPhone
  - Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3 like Mac OS X; en-gb) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8F190 Safari/6533.18.5

How to detect LAN devices

4. Check the used applications

- 有些 things/devices 沒有 Ethernet/Wifi，必須透過 (IoT) Gateway 轉換通雲端 (to log servers)。
  - 看不到 MAC address, DHCP options 55, 不一定有 user-agent
  - 傳統招式：
    - IP、domain name、traffic or string-based patterns.
    - 還是要想法子識別

How to detect LAN devices

4. Check the used applications

- AppID
  - 1. 關於一般 pattern-based AppID
  - 2. AppID for SSL-based applications
  - 3. AppID for encrypted applications

How to detect LAN devices

4. Check the used applications

- 關於一般 pattern-based AppID
  - 主要是AppID會希望 connections 能夠被儘早的識別出來並標注適當的ID ，這樣可以及早 apply QoS
  - IPS則是必須在關鍵時刻擋下攻擊，在高速網路(一秒鐘幾十G上下)的環境，就會變得很刺激

How to detect LAN devices

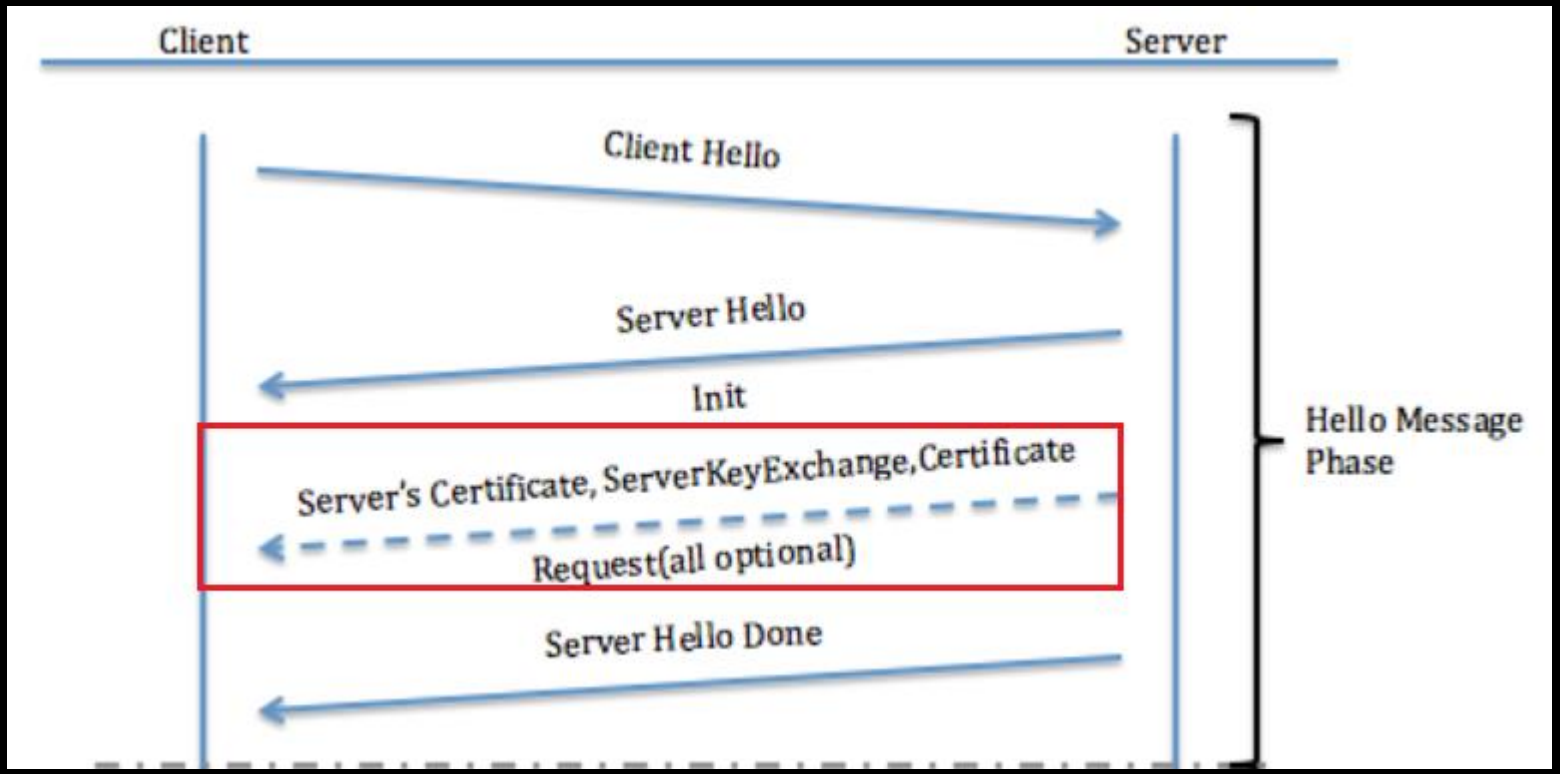
4. Check the used applications

- AppID for SSL-based applications
  - 有些人遇到 SSL 的連線就放棄識別了， but

How to detect LAN devices

4. Check the used applications

- AppID for SSL-based applications

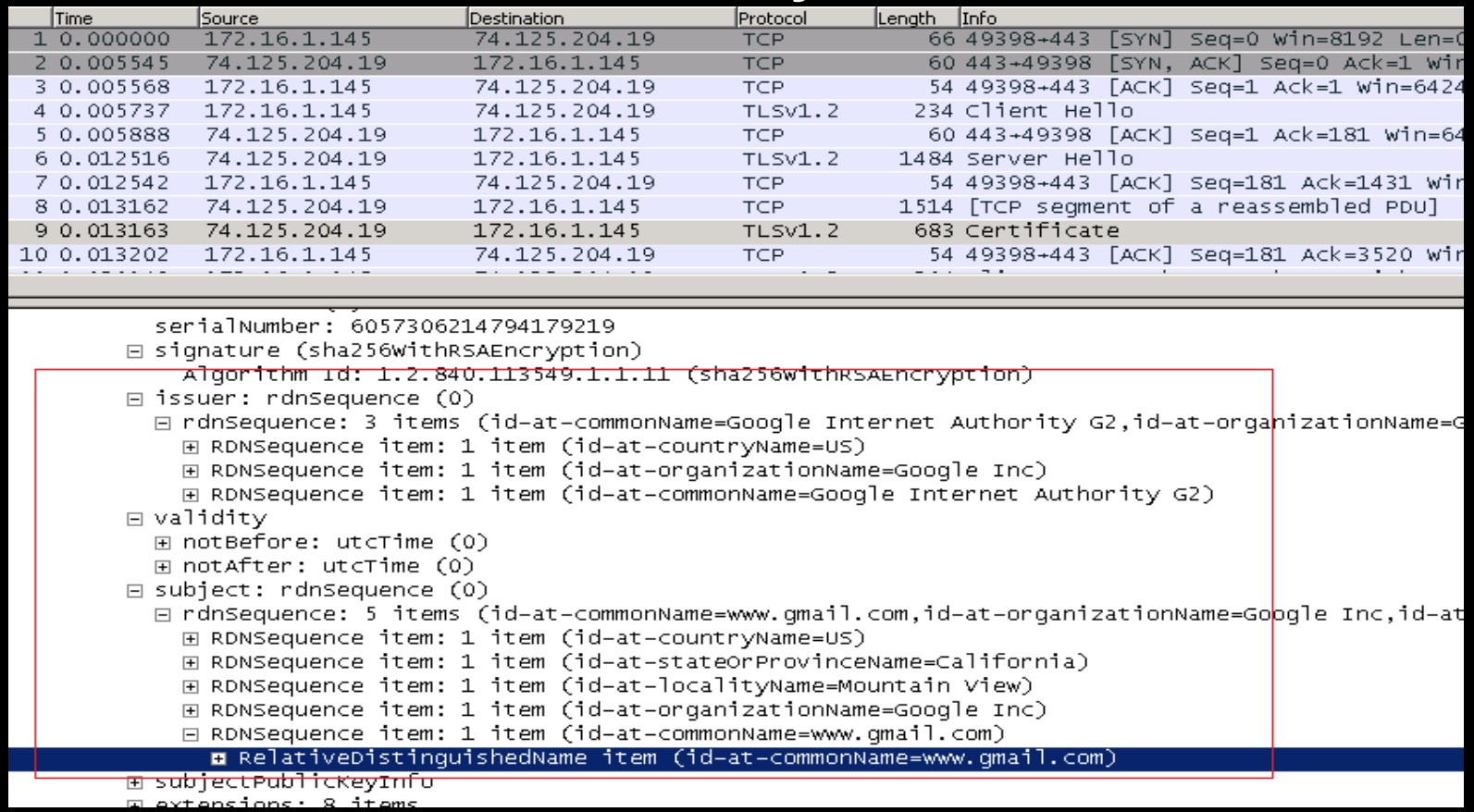


- Source: http://www.cisco.com/c/en/us/support/docs/security-vpn/secure-socket-layer-ssl/116181-technote-product-00.html

How to detect LAN devices

4. Check the used applications

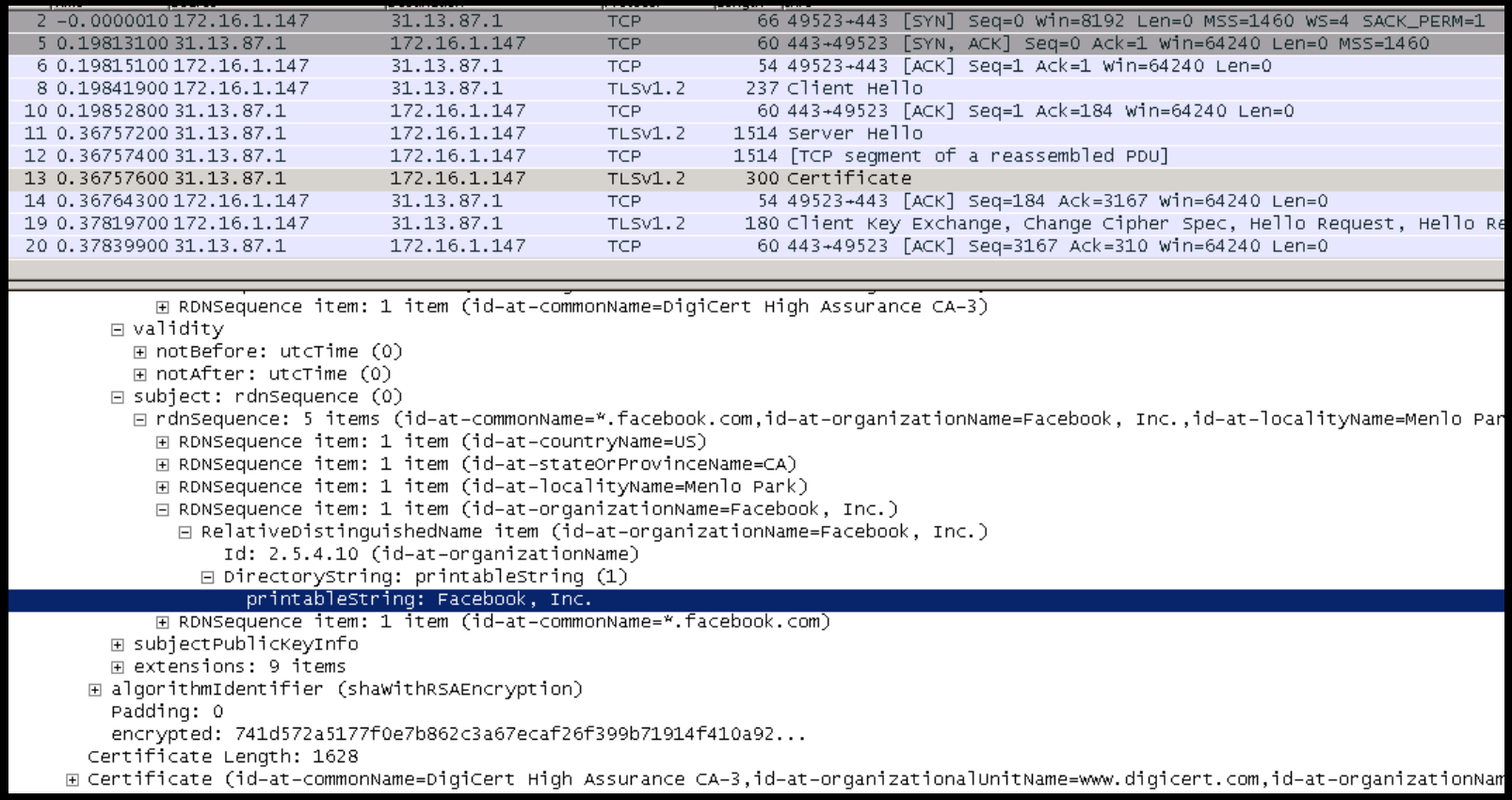
- Certificate 裡面有些 keywords 可以抓
-



How to detect LAN devices

4. Check the used applications

- Certificate 裡面有些 keywords 可以抓
-



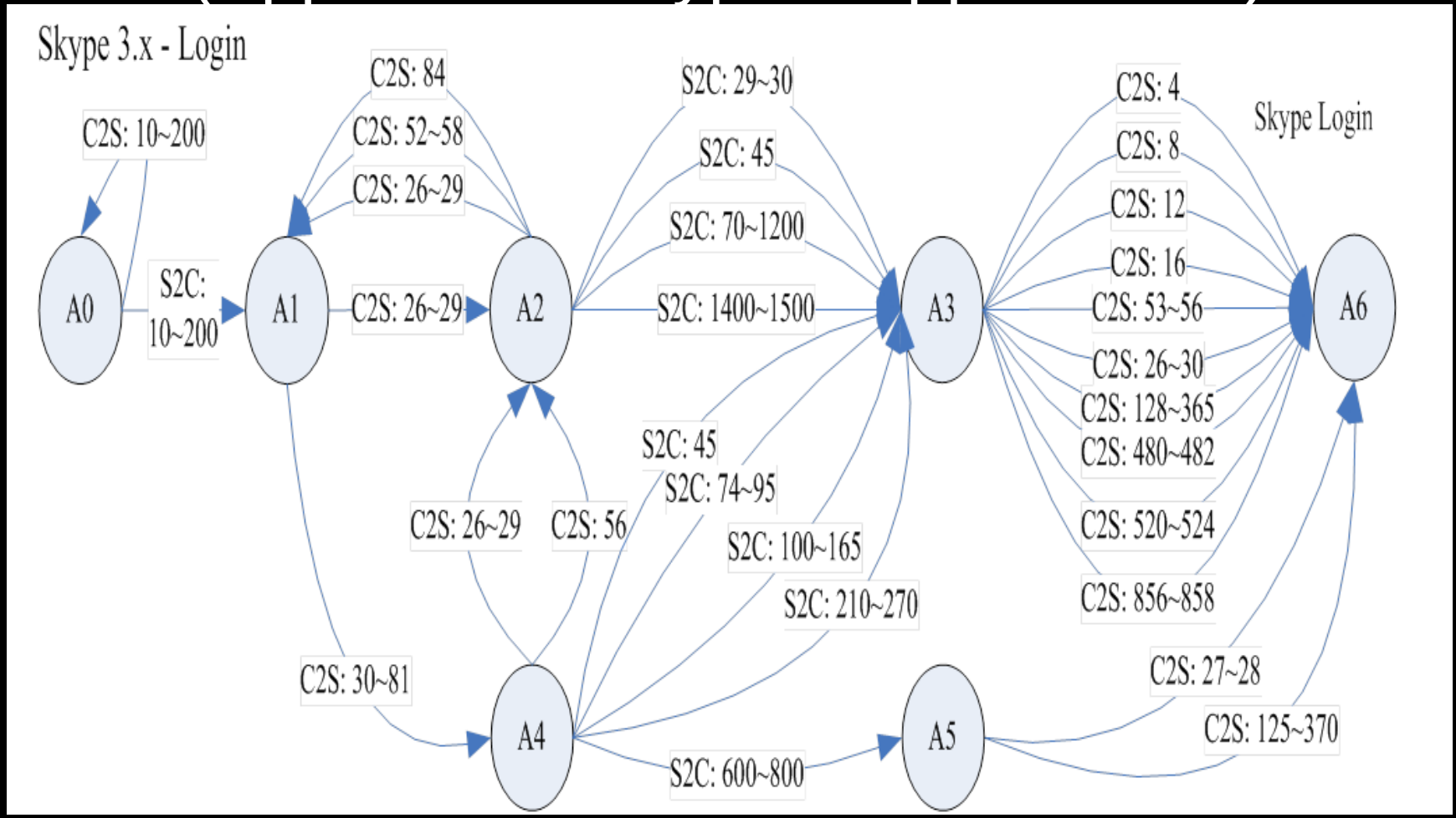
How to detect LAN devices
4. Check the used applications
(AppID for encrypted applications)

- 如果，你遇到的是私有的加密方式或編碼，無法知道封包的解析規則
  - 那還有招嗎？

How to detect LAN devices
4. Check the used applications
(AppID for encrypted applications)

- 那我們提供一個沒有辦法的辦法
  - 放棄識別 payload
  - 單靠 方向、封包長度，產生出對應的 finite state machine (FSM)
  - 如果，這個 FSM 可以 match 某個 connection，我們就假定它應該跟我們用來畫出這個 FSM 的 connections 是同一種。

How to detect LAN devices
4. Check the used applications
(AppID for encrypted applications)



How to detect LAN devices

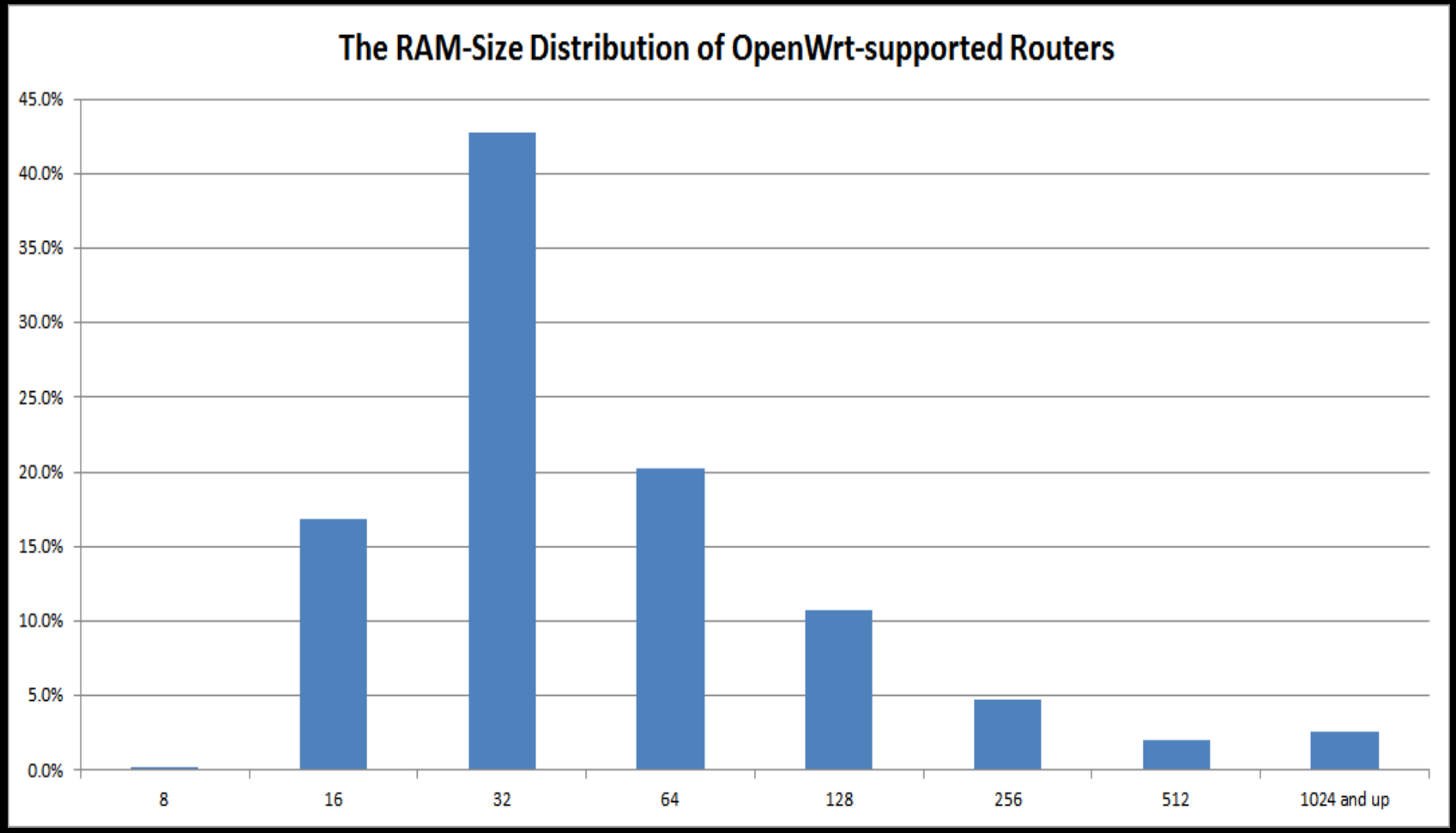
- 誰適合做 LAN Device Identification?

- IoT Home Router/Gateway?
  - 兵家必爭之地？
  - LAN 與 WAN 資料交換必經之路
  - 一般來說，真正的 source MAC address 與 DHCP option 55 只有在 LAN 看得到。

How to detect LAN devices

- Do you know the RAM-size in your home router?
  - 你知道家裡的 router 的 RAM 是多大嗎？
  - In embedded system, in general, the RAM-size imply the functionality which can be equipped.

How to detect LAN devices



How to detect LAN devices

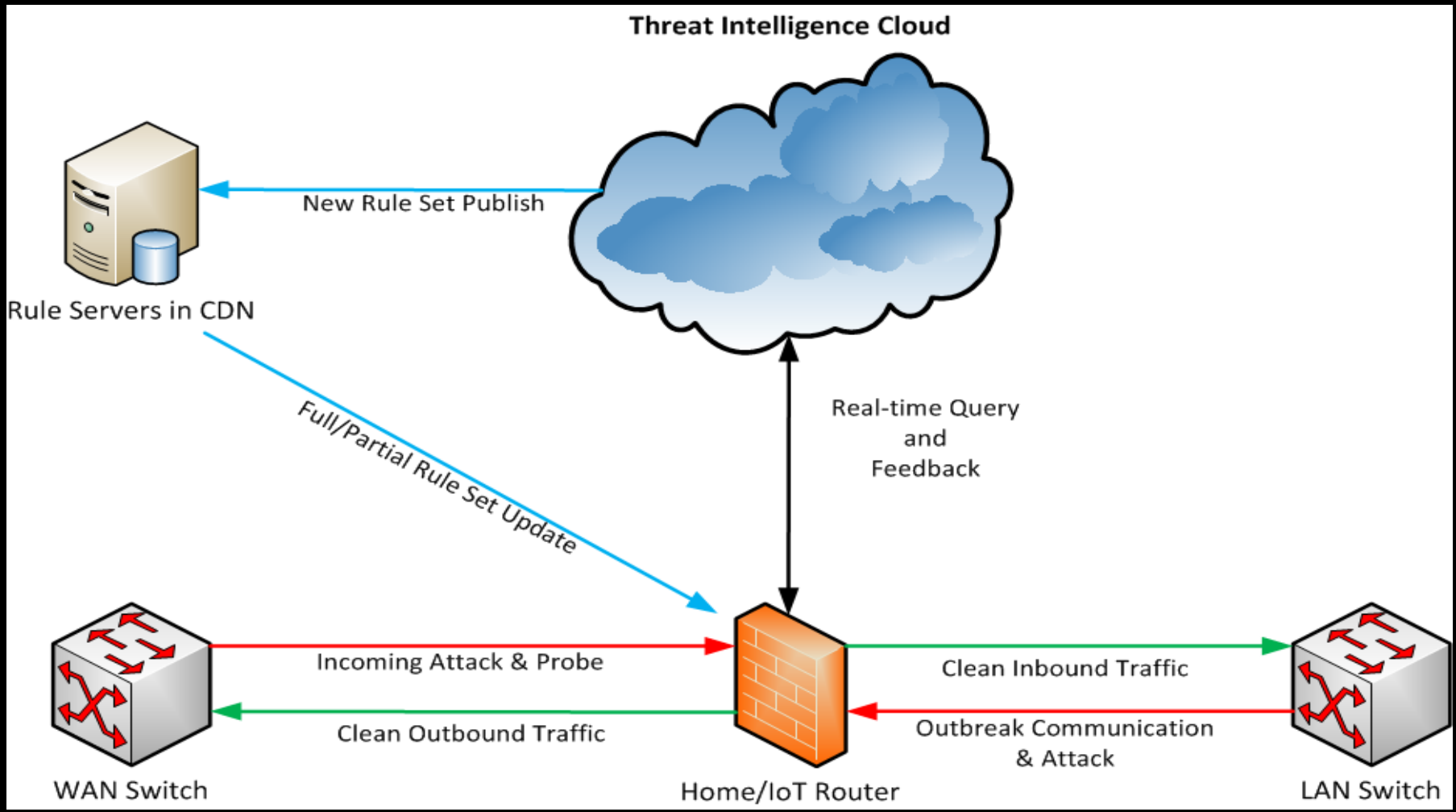
- 當大部分的家用 router 的 RAM 少於 128M，(32M 是主流)，大家覺得它會拿多少出來給 security functions?
  - 無米之炊....
  - 這是大環境的問題，需要大家一起解決。
  - Security has its price.

- The threat intelligence with LDI

The threat intelligence with LDI

- 我們和 home router 廠商合作，取得 user 同意的 logs，彙整到我們的 cloud。
  - Timely
  - Accurate
  - Relevant

The threat intelligence with LDI



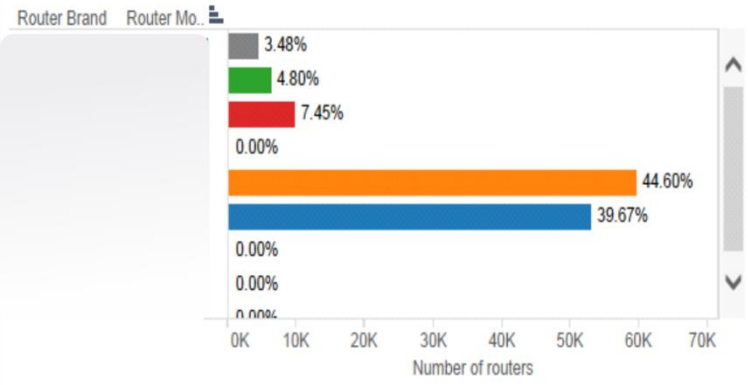
The threat intelligence with LDI

- 底下是一些去可識別化的統計資訊

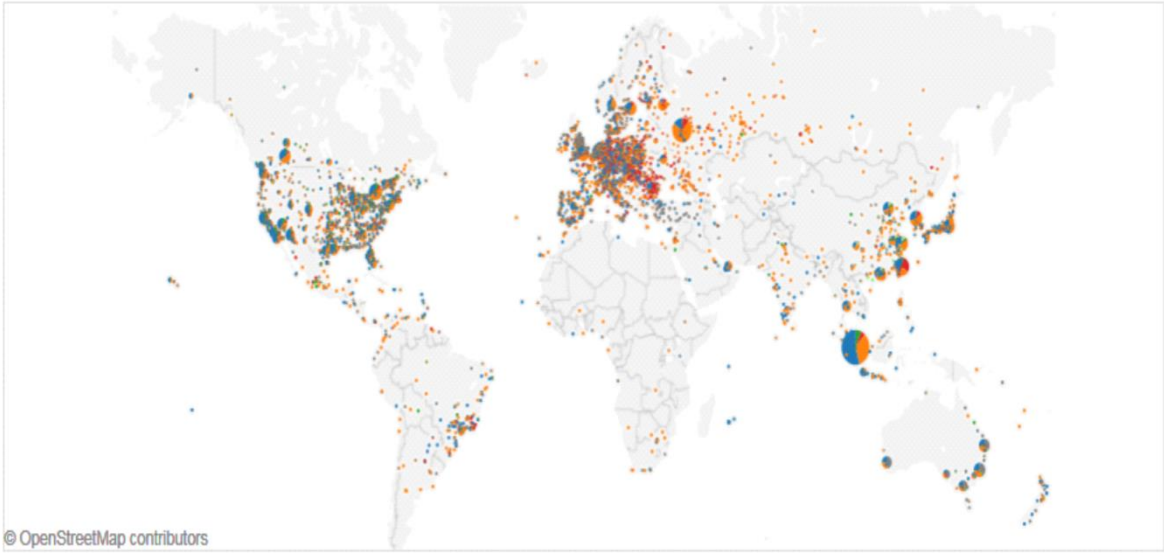
Summary

Number of routers	134,869
Number of devices	2,834,241
Number of events	2,107,087

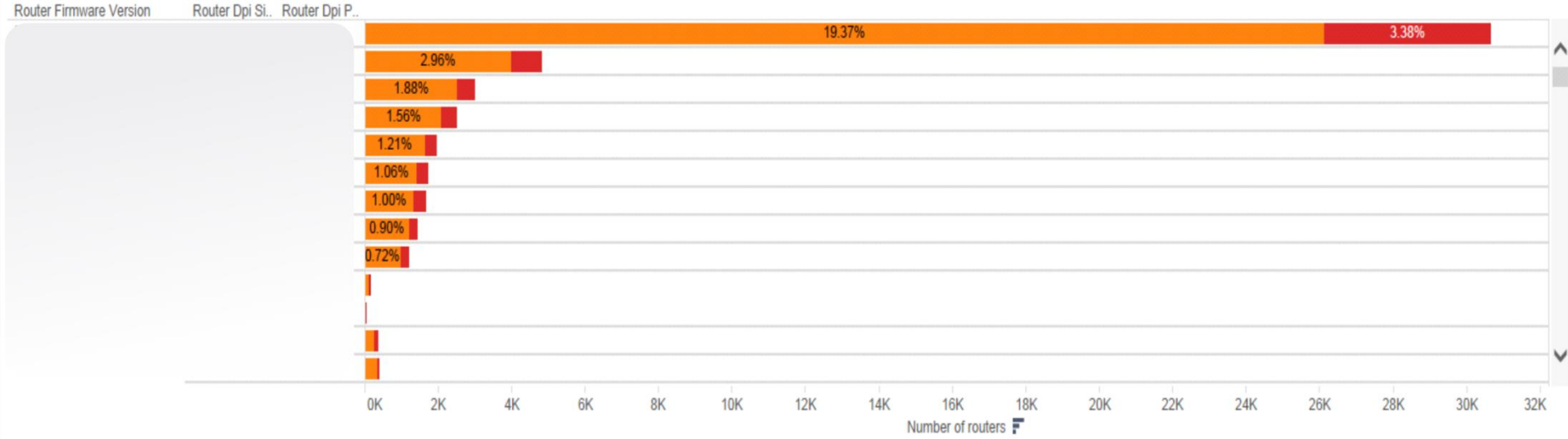
Router Model



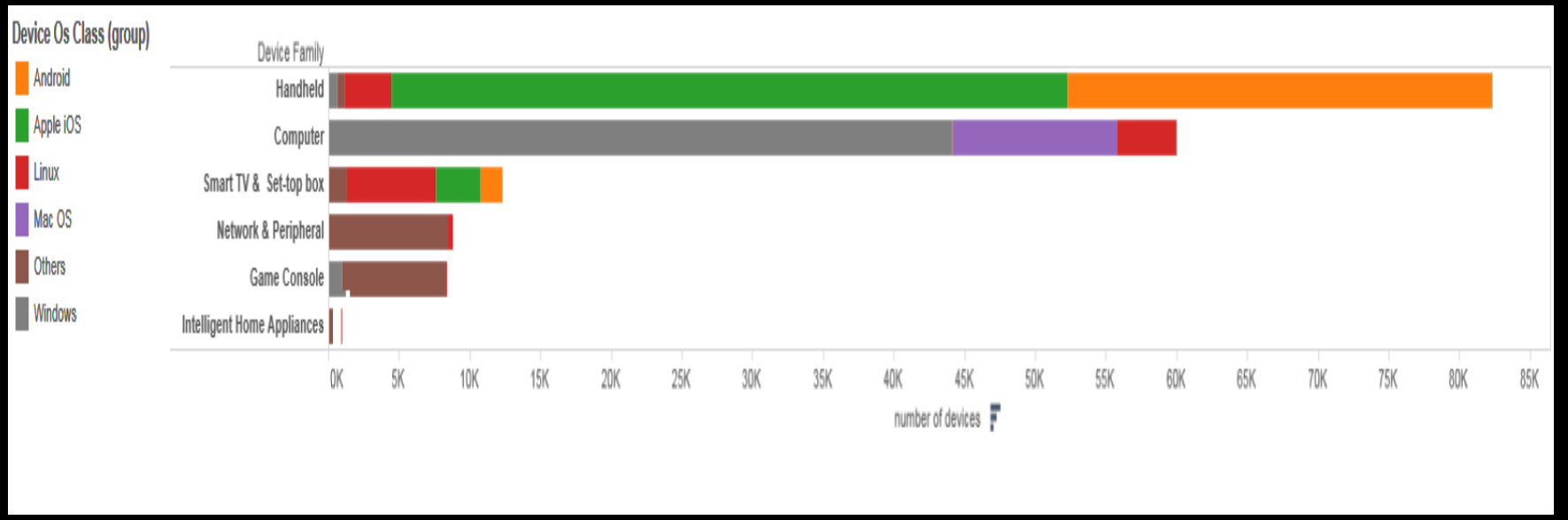
Routers on the map



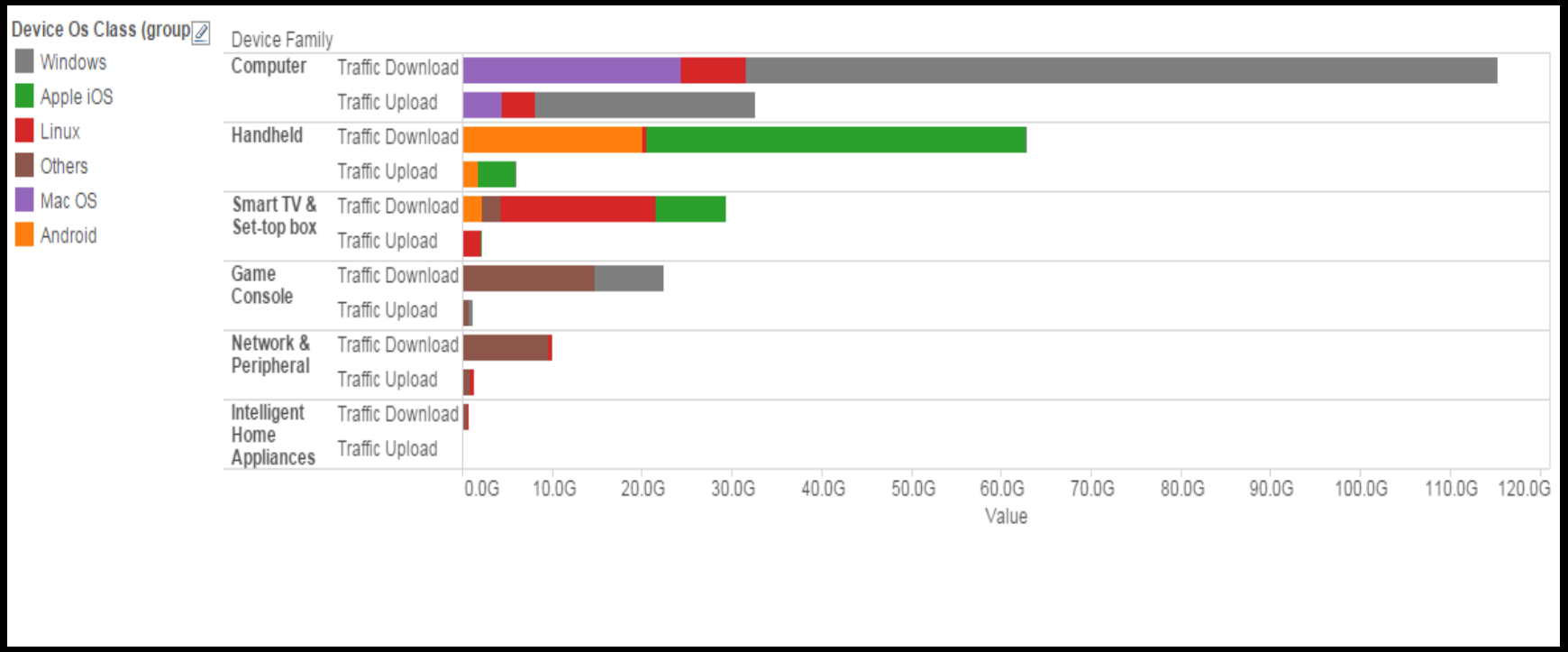
Router Version



The threat intelligence with LDI
Device by type

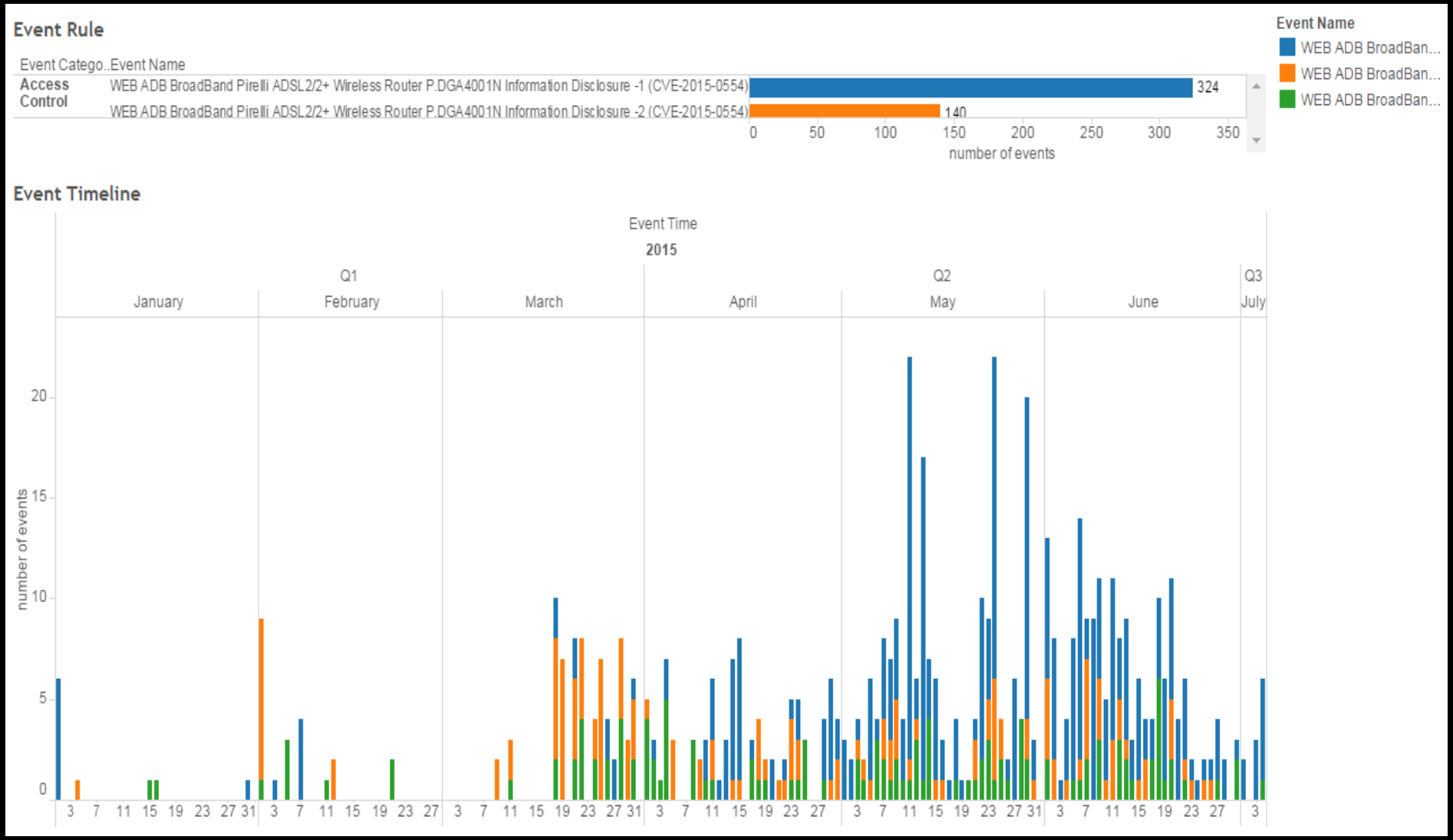


The threat intelligence with LDI Traffic by Device

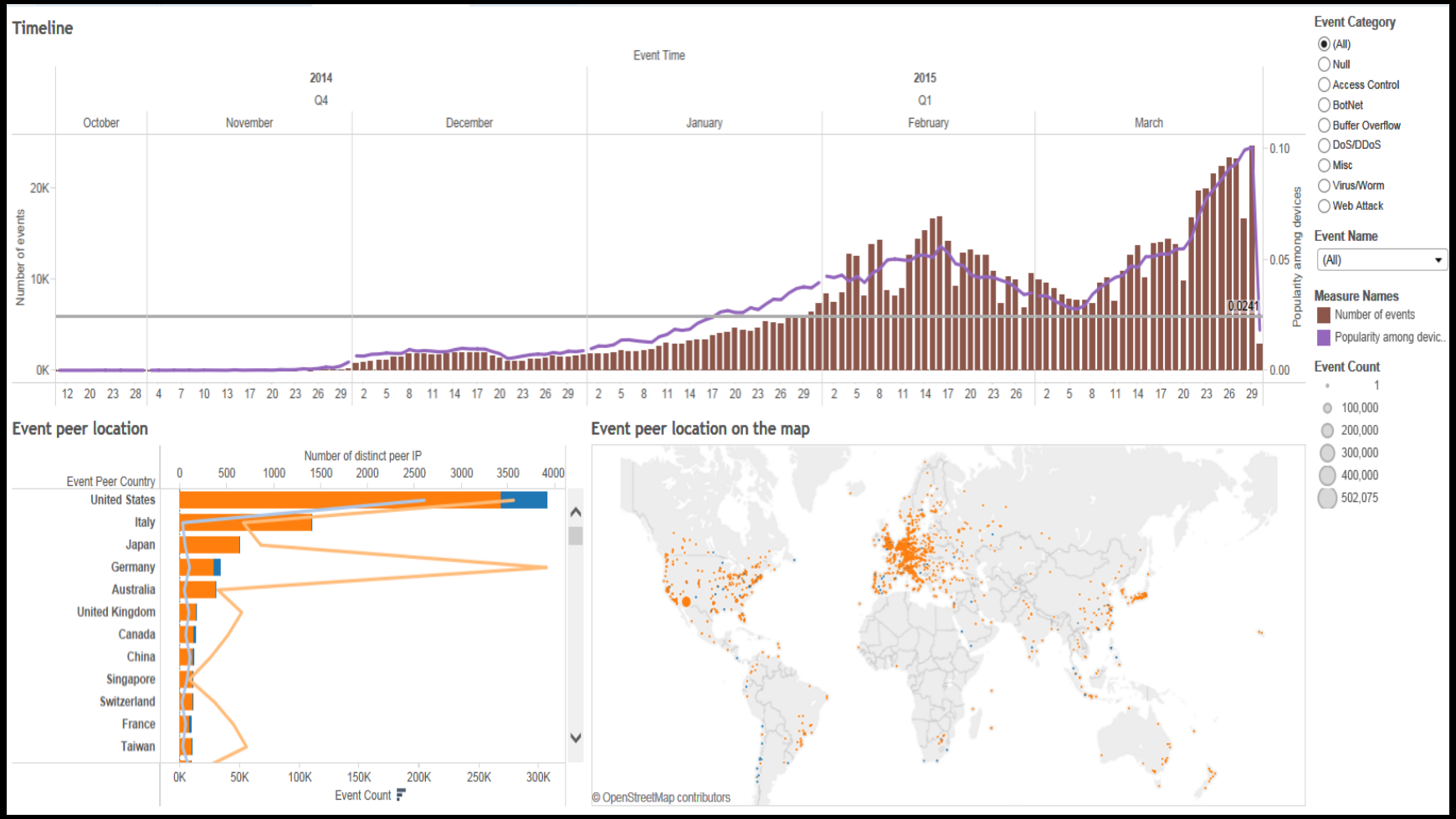


The threat intelligence with LDI

CVE 2015-0554 (Release Date: 2015/1/21)



The threat intelligence with LDI Security Events timeline



The threat intelligence with LDI

- 第二屆台灣資料科學愛好者年會
  - 阿里巴巴數據委員會會長-車品覺：
  - 數據科學現在有兩大派別：
    - 數據很平但用深厚的演算法解決問題，
    - 另一種是數據廣泛而大但是用簡單的演算法。
    - 我(車品覺)個人的喜好是第二個 ☺

The threat intelligence with LDI

- 我們也是喜歡簡單的演算法 ☺
- 再回到那個冰箱送 SPAM 的問題
  - 萬一，我們發現你家的冰箱開始送 emails
  - 我們會比對別人家的同款的冰箱們是不是也會送 emails
  - 如果，你家的冰箱是特別的
  - 理論上，將來我們會想法子通知你....
    - ~~自己的冰箱自己救~~

- Summary

Summary
(Some things about LAN device identification)

- 1. 在 IoT 時代，網路設備識別自動化是需要的。
- 2. 在 LAN 端，我們可以透過 MAC OUI，DHCP packets 取得品牌與作業系統的相關資訊。
- 3. 精準的設備識別 結合 Big Data 的運算能力，才有辦法真正做到 threat intelligence。

Acknowledgements

- The Authors would like to thank
  - Eric Lien
  - MiG Chien
  - Hubert Lin
  - Ping-Jhih Chen
  - Miles Xie
  - Mit Liao
  - Justin Jan
  - and other helpers.

Reference

- 1. MAC address
  - https://en.wikipedia.org/wiki/MAC_address
- 2. Fingerbank
  - https://fingerbank.inverse.ca/
- 3. Using DHCP for Passive OS Identification
  - http://chatteronthewire.org/download/bh-japan-laporte-kollmann-v8.ppt
- 4. Packetfence
  - http://www.packetfence.org/

One more thing

(在 HITCON2015 ENT, 兩個 hackers 的問答)

- 安東尼問：
  - 我們一直揭露偵測與防禦的技術，會不會造成壞人一直改進，使得我們偵測與防禦的能力變弱？
- 博德曼答：
  - 不用擔心這個問題，因為我從來沒有在公開的演講，揭露我真正的實作方法與技術 ☺
- Comments:
  - 也不是說我們這些 speakers 都留一手，而是說我們做的比說的好 ☺

Q&A

- Thank you ☺

- E-mails:
  - For media and business
    - Terence Liu <terence_liu@trend.com.tw>
  - For job opportunity
    - Hsien-Wei Hung <hsienwei_hung@trend.com.tw>
  - For technique
    - Canaan Kao <canaan_kao@trend.com.tw>

About BoT2015

- 現狀：
  - 我現在還不能跟大家確認今年不會有 BoT2015
  - 大概九月底會有 update
- Facebook for BoT conference:
  - https://www.facebook.com/BotnetCon