MAC randomisation – considering privacy features with potential unintended network consequences

Plus a quick update on DoH and ECH

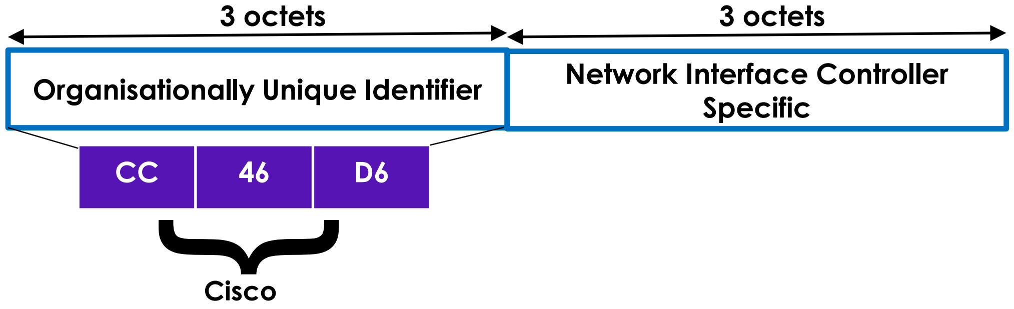
UKNOF 20th July 2020

Andy Fidler, Simon Ringland, Paul Woodward

Background – The history behind MAC addresses

- A Media Access Control (MAC) address is a unique identifier assigned to a network interface controller, e.g. Wi-Fi or Ethernet.

- It takes the format of a 48-bit address
  - the first 3 octets identifying the device manufacturer through an Organisationally Unique Identifier
  - the latter 3 octets identifying the specific network interface controller, e.g. unique to the device.


3 octets
3 octets
Organisationally Unique Identifier
Network Interface Controller Specific
CC
46
D6
Cisco

- It is standardised by the IEEE, and is visible unencrypted in Wi-Fi polling and connection handshakes.

- To enhance privacy IEEE, Applications and Operating Systems have started to introduce various forms of randomisation.

- Like other internet protocols, ISPs have found many wider uses of MAC addresses, e.g. automatic Wi-Fi connection, access control and customer support.

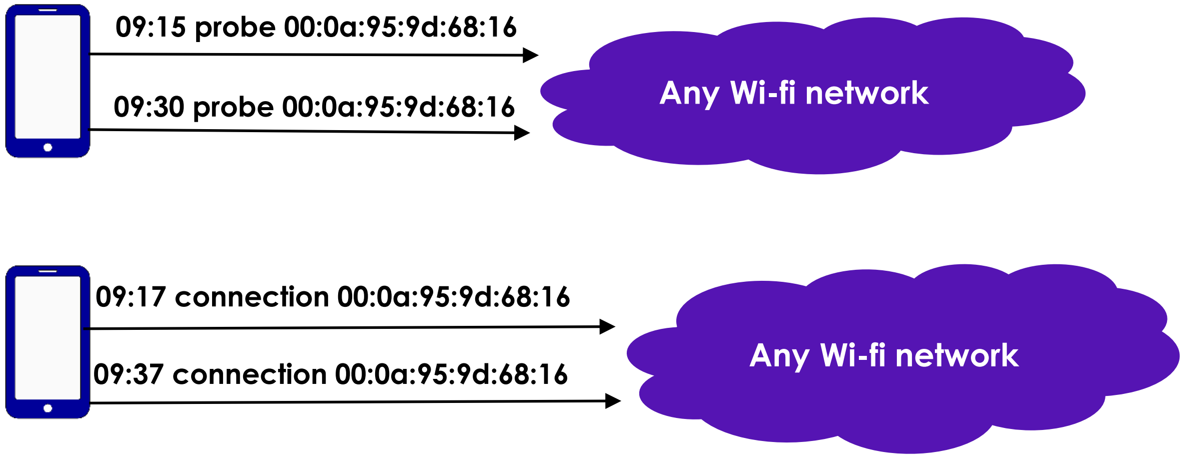
- This presentation outline thoughts on balancing MAC randomisation privacy features with potential unintended consequences on the network and customer experience.

- Focussing on the main impact area – Wi-Fi connectivity.

MAC address evolution – Phase 0 No Randomisation

- Mainly legacy devices

- Always use the same permanent MAC address for both Wi-Fi polling / probe requests and connectivity.



09:15 probe 00:0a:95:9d:68:16

09:30 probe 00:0a:95:9d:68:16

Any Wi-fi network

09:17 connection 00:0a:95:9d:68:16

09:37 connection 00:0a:95:9d:68:16

Any Wi-fi network

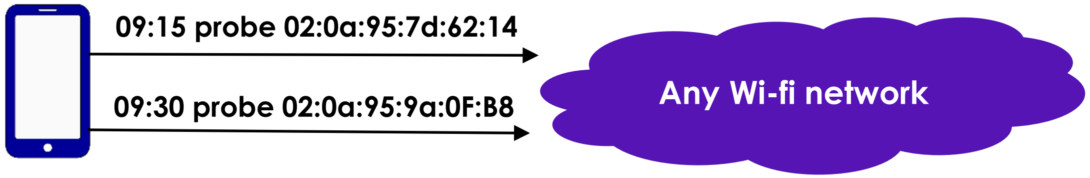
- No privacy through randomisation

- No impact to existing ISP networks and customer service.

MAC address evolution – Phase 1 Probe Randomisation only

- Some devices

- Random MAC addresses for each probe request to offer some form of privacy

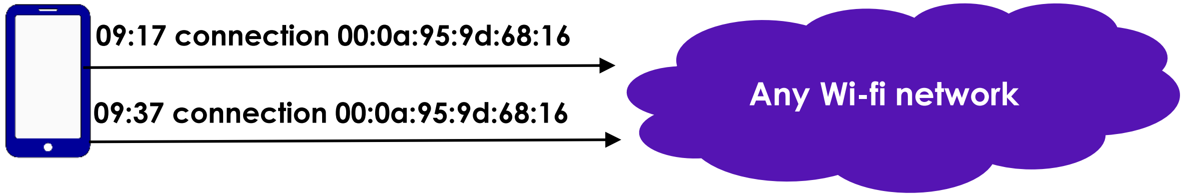


09:15 probe 02:0a:95:7d:62:14

09:30 probe 02:0a:95:9a:0F:B8

Any Wi-fi network

- But still uses permanent MAC address for Wi-Fi connections.



09:17 connection 00:0a:95:9d:68:16

09:37 connection 00:0a:95:9d:68:16

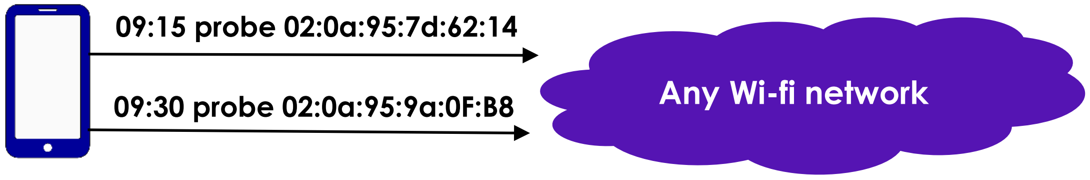
Any Wi-fi network

- No impact to existing ISP networks and customer service as same MAC address always used per connection.

MAC address evolution – Phase 2 Probe + per SSID randomisation

- Latest devices and Operating Systems.

- Random MAC addresses for each probe request

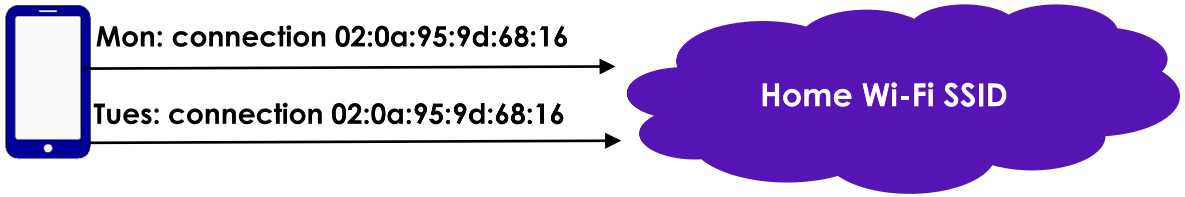


09:15 probe 02:0a:95:7d:62:14

09:30 probe 02:0a:95:9a:0F:B8

Any Wi-fi network

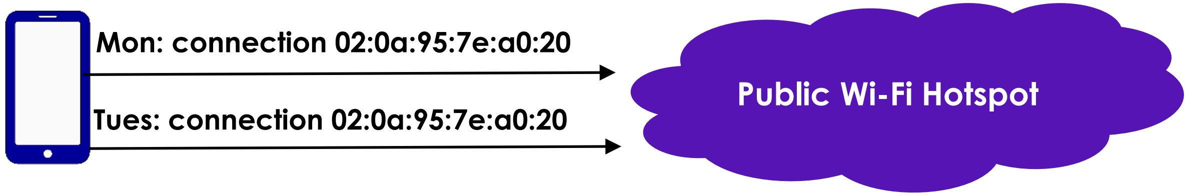
- Plus for added privacy different MAC addresses for connection on a per SSID / realm basis, but re-used for subsequent connections.



Mon: connection 02:0a:95:9d:68:16

Tues: connection 02:0a:95:9d:68:16

Home Wi-Fi SSID



Mon: connection 02:0a:95:7e:a0:20

Tues: connection 02:0a:95:7e:a0:20

Public Wi-Fi Hotspot

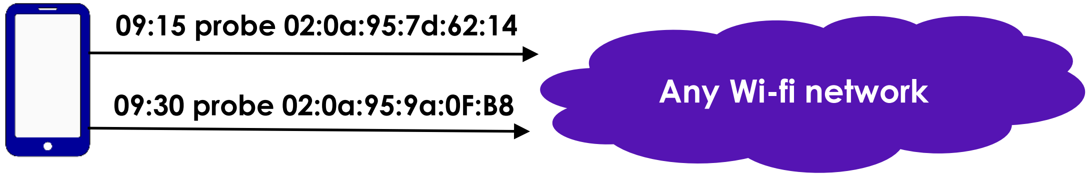
- No impact to existing ISP networks and customer service as same MAC address always used for same SSID connection.

MAC address evolution – Phase 3 Probe + per session/day randomisation

- **Option exists now in Microsoft Windows 10.**
  - https://support.microsoft.com/en-us/help/4027925/windows-how-and-why-to-use-random-hardware-addresses

- **Apple announced through developer conference their plans around Private Wi-Fi in iOS 14.**
  - https://developer.apple.com/videos/play/wwdc2020/10676/ Private Wi-Fi update starts at 21:30

- **Random MAC addresses for each probe request**

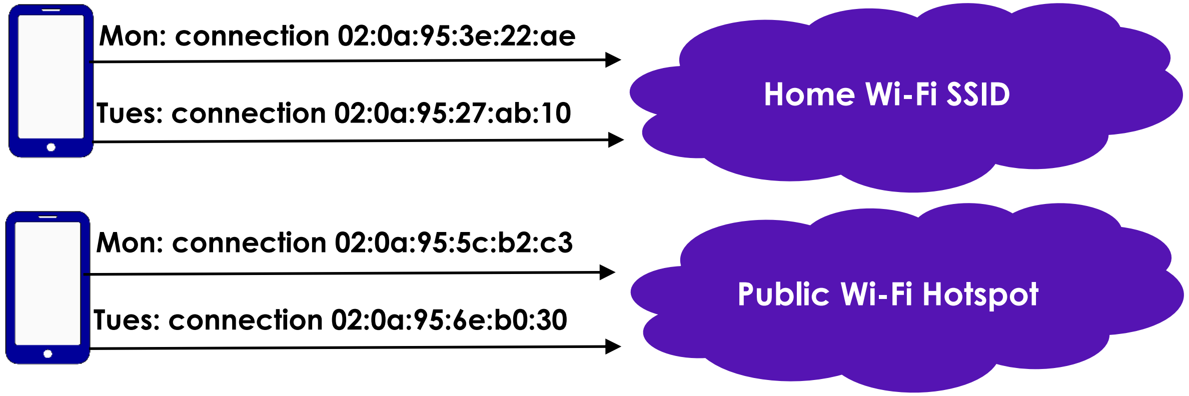


09:15 probe 02:0a:95:7d:62:14

09:30 probe 02:0a:95:9a:0F:B8

Any Wi-fi network

- **Plus for FULL privacy randomised MAC addresses for connection on a per session basis / per day / per network SSID.**



Mon: connection 02:0a:95:3e:22:ae

Tues: connection 02:0a:95:27:ab:10

Home Wi-Fi SSID

Mon: connection 02:0a:95:5c:b2:c3

Tues: connection 02:0a:95:6e:b0:30

Public Wi-Fi Hotspot

- **Maximises privacy, but risks creating unintended consequences to customer experience and support.**
  - **For example impacts to public hotspot seamless MAC authentication, time of day access controls, device based parental controls and regulatory obligations.**

Per Session MAC randomisation impact areas & mitigation options

Area	Impact	Mitigation Options
Public Wi-Fi Hotspots	• Breaks MACs authentication journey used by many public Wi-Fi hot spot providers to allow seamless connection after initial registration. • Impacts any network diagnostics based on device MAC address.	• Move to use of Wi-fi Passpoint / 802.1X but this may require additional user interaction in terms of accepting certificates / profiles and provisioning journey for non-SIM devices.
Broadband: Customer Support	• Potential inability to identify device make, model and number of devices connected at home to aid customer contact troubleshooting. • Impacts Home Wi-Fi diagnostic capabilities. • May impact future device steering between access points and bands (2.4GHz / 5GHz)	• Longer term use of any new IEEE 802.11 physical layer identifiers. • Wi-fi Alliance – Wi-fi Certified Easy Connect (DPP) capabilities where it uses per device specific connectors. • Per device passwords to identify devices, but needs automatic password provisioning solution, e.g. DPP. • In theory Wi-fi Passpoint but need to consider provisioning journey aspects. • For some devices DHCP friendly name may be unique within the home, e.g. Joe's iPad – could potentially use this, but only as a partial solution.
Broadband: Access Controls & Content Filtering	• Breaks per device time of day access controls in home equipment as many of these are based on MAC address. • Breaks any per device broadband parental controls based on MAC addresses.	

Current focus on laptops, tablets and smart phones what are the additional impacts if rolled out to IoT devices?

Next steps, if your services could be impacted by MAC randomisation

- **Read background to MAC randomisation from IEEE RCM TIG working group**
  - https://mentor.ieee.org/802.11/dcn/19/11-19-0588-01-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt
  - https://mentor.ieee.org/802.11/dcn/19/11-19-1442-09-0rcm-rcm-tig-draft-report-outline.odt

- **Check out Apple and Microsoft information**
  - https://support.microsoft.com/en-us/help/4027925/windows-how-and-why-to-use-random-hardware-addresses
  - https://developer.apple.com/videos/play/wwdc2020/10676/ Private Wi-Fi update starts at 21:30

- **Identify your service and support dependencies on MAC address and mitigation options**

- **Engage in a potential new IEEE 802.11 Task Group covering MAC randomisation and wider Wi-Fi security**
  - https://mentor.ieee.org/802.11/dcn/20/11-20-0990-01-0rcm-security-and-privacy-maintenance-task-group-par-ideas.pptx

- **Talk to your Operating System contacts**

Encrypted DNS and ECH developments to check-out

- **Apple Developer Conference videos on privacy and encrypted DNS**
  - https://developer.apple.com/videos/play/wwdc2020/10676 timestamp 11:55
  - https://developer.apple.com/videos/play/wwdc2020/10047/

- **IETF Encrypted Client Hello (ECH)**
  - https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
  - **Addresses fact that HTTPS still shows site name at the start of every connection.**

- **Encrypted DNS and ECH have the potential to cause unintended consequences to:**
  - **Existing ISP DNS and packet inspection based content filtering (parental controls, malware protection & regulatory/court order)**
  - **Network cyber security intelligence**
  - **ISP use of local on-net content caches**
  - **ISP / Network Operator Customer troubleshooting**
  - **Zero rating, the ability to identify and classify known content/services to exclude from usage-based charging**

- **Encourage ISP/Operators to review impacts and engage in OS, Industry Alliances and IETF discussions**

Conclusion

- BT looks favourably on new capabilities that enhance privacy and security for our customers.

- However whilst increasing privacy, further MAC randomisation risks creating unintended consequences to customer experience and support.
  - For example impacts to public hotspot seamless MAC authentication, time of day access controls, device based parental controls and regulatory obligations.

- In a similar way Encrypted DNS and ECH privacy comes with impacts to existing content filtering, zero rating and customer support capabilities.

- BT would welcome continued industry dialogue on balancing these emerging privacy features with unintended consequences on network and customer experience.

BT