MADINAS Use Cases

Simon Ringland (BT)

Rajat Ghai (Comcast)

Ian Wheelock (Commscope)

Mohamed Boucadair (Orange)

Malay Vadher (Plume)

Ajay Manuja (Benu Networks)

Access Control based on MAC Addresses

- CPEs widely support filtering features based MAC addresses
  - An additional guard for access control such as accept- or discard-lists
- Example services:
  - ISPs use MAC address filter to mitigate DDoS at the L2 edge. Filtering based on the IP address at the network side is suboptimal
  - Schedule when a device can be granted access (e.g., parental control)
  - Seek a confirmation from an administrator when a new device is detected

Sticky DHCP Assignment for Incoming Connections

- CPEs provide DHCP server service
- It is quite common that users rely upon a sticky DHCP to assign a static IPv4 address to a given device for various functions:
  - DMZ
  - (Static) Port Forwarding

DHCP Address Pool Exhaustion

- Clients connecting with different MAC addresses are assigned new DHCP IP addresses
- Normally a DHCP Server maintains a single IP address for a client
- With MAC Randomisation, the DHCP Server has to assign a new IP address every time a client changes its MAC address
- IP Address exhaustion at the DHCP server may prevent clients from joining a network as no more addresses free to assign
- If customer network equipment is limited to a maximum number of MAC addresses, this may be exhausted due to MAC randomisation

Diagnostics

- ISPs need to be able to provide remote support for their customers to help identify and diagnose problems that the customers are having with their connectivity.
- There is a need to be able to identify the current performance and behaviour of each individual device and to understand the patterns of performance of each device over a period of time that extends to at least several weeks.
- Thus there is need for a persistent device identifier.
  - For most diagnostics purposes the identifier only needs to be unique and persistent within an individual home network (ESS).
  - However, there exist some diagnostics examples (such as detecting when a device has mistakenly connected to the community Wi-Fi side of an access point rather than the private LAN side), where an identifier that is common across different ESSes would be required.
- ISPs also need to be able to discuss the performance of specific identified devices with the customer and so need to be able to tie the diagnostic device identifier to a device name or description that the customer will understand.

Enhanced Features for Home Networks

- A device in home is associated to a family member profile using the device's MAC address
- Following features are based on the family profile (affected by MAC address randomization):
  - Security and content access policies (e.g., Adult content access restriction on a child device)
  - Pause or freeze schedules (e.g., Dinner time or Bedtime internet restriction for family members)
- Device nicknaming, person or room assignment is also lost

Cloud Resource Management

- A device record is stored in cloud for management of various features (family profile, service policies, steering, etc.)

- The size of the record database increases astronomically as the device MAC address change frequency reduces. For example:
  - For one month period, if the MAC address of each home client changes every 24 hours, then database size is 30X more than that of one where no device randomized MAC address once associating to the network

- This also results in increase in complexity of database management as well as other essential cloud components referring the device records

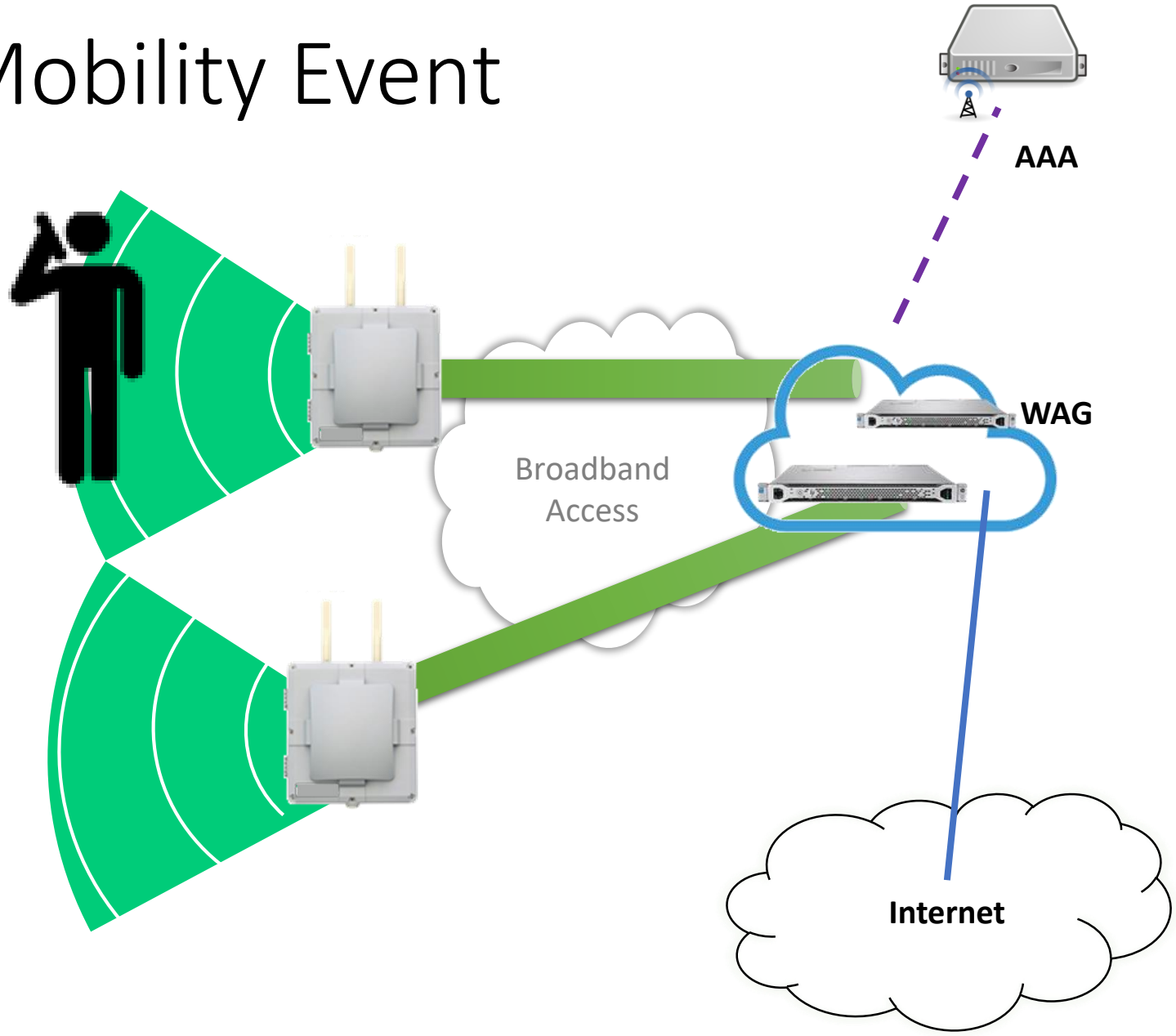
Community Wi-Fi Auto Sign-in

- Many ISPs offer an open and secure SSID as a public Wi-Fi service to their customers across millions of APs

- Many users access public Wi-Fi service using the open SSID
  - First time authentication of a user is done via username/password provided by the supplicant
  - Once the identity of the user is confirmed and verified the network caches the MAC address of the supplicant for provide auto auth to return users, until cache expiry.

Community Wi-Fi Mobility Event

- New Device onboarding
  - AP tunnels all traffic to WAG
  - Portal or MAC based Auth via AAA
  - WAG Assigns local IP Address and NAT ports
- Mobility Event: UE move between APs
  - UE MAC is matched to detect the tunnel switch at WAG
  - UE IP and NAT state is switched to new AP
- Different MAC from same UE
  - Restart of device onboarding and Authentication process
  - Reset of all existing connections and NAT pool
  - Possible service denial attack If MAC address is not checked



QoE Measurement & Improvement

- Some Community Wi-Fi providers do continuous measurement of Quality Of Experience (QoE) of their users on the Wi-Fi network by scoring the QoE

- Correlation of QoE experiments pre/post network tuning relies upon a persistent device identifier (MAC). For example:
  - Device MAC “A” had a QoE score of “X”
  - Operations team tunes that segment of the network, soak changes
  - After Y days, QoE measurements are performed for device MAC “A” , and QoE score of “Z” is observed

Legacy Client Steering and Pre-Association Steering

- While the new MBO based client steering relies on devices reporting their view on the signal strengths of access points, legacy mechanisms rely on access points making measurements of the signal strength of clients.
- For such solutions, access points may have to compare the signal strength they see on a probe request on one band with the signal strength they see for data traffic of the same station that is associated on another band.
- If the probe request uses a different MAC address than is used for the associated connection, then the access point will be unable to determine that the probe request is from the same device and will therefore be unable to perform the client steering action.
- Furthermore, APs may need to record which clients do not respond well to legacy steering attempts in order to avoid repeating the same poor experience. This requires a persistent identifier for the client device.
- Pre-association steering may also be affected, depending on the specific implementation, as client devices using MAC randomisation may use one MAC address for probing and a different one for association.

Use Cases – Summary

- Today many services rely on the device MAC address being a persistent identifier
- The consequence of the introduction of MAC randomisation is that these services will stop working
- Some may be fixed by tweaking the implementation, but not for most of the use cases
- Alternative identity solutions are required to enable the services to continue to operate whilst preserving user privacy

Use Case-derived Requirements

Requirements

- Different use cases have different requirements on an identity, so a number of different solutions may be required.
- Key features to consider for each case are shown in the table to the right ==>

Example Use Cases

- Access Control
- Sticky DHCP Assignment
- DHCP Address Pool Exhaustion
- Enhanced features for home network
- Diagnostics
- Cloud Resource Management
- Community Wi-Fi Auto Sign-in
- QoE Measurement & Improvement
- Legacy Client Steering
- Pre-Association Steering

Feature	Description
Persistence	How long must the identifier persist?
Security & Trust	What level of trust is required between the client and the network and how confident must the network be that the client is the true owner of the identity?
Pre-Association Security & Trust	Is the same identifier required to be used pre- and post-association?
Single, multiple or all SSIDs	Is the same identifier required on a single network (ESS) or multiple networks?
Device or User	Does the identifier represent the device or the user?
Mandatory or user opt-in	Must the identifier be provided in order to join the network, or must the user opt-in?
Provisioning	The provisioning of any new identifier must be low-friction for the user. How could this be achieved?