IEEE 802.11u Overview

Klaas Wierenga

TF-Mobility

Loughborough, May 7, 2009

802.11u Executive Summary

- 802.11u – Interworking with External Networks
- Purpose:
  - –Interworking with External Networks is a key enabler to allow IEEE 802.11 devices to interwork with external networks, as typically found in hotspots or other public networks irrespective of whether the service is subscription based or free.
  - –Interworking Service aids network discovery and selection, enabling information transfer from external networks, and enabling emergency services. It provides information about the networks prior to association.
  - –Interworking Service addresses MAC layer enhancements that allow higher layer functionality to provide the overall end-to-end interworking solution.
- Timeline:
  - –Currently in re-circulation Letter Ballot
  - –Expected start of Sponsor Ballot, July 2009
  - –Final 802.11 working group approval: January 2010
  - –Final ratification by 802: June 2010

Problems Related to Network Discovery and Selection

- Terminal powers up in urban setting and scan environment—finds ~100 Wi-Fi networks. How should it select the right network without depleting its battery?
- Terminal doesn't recognize SSID, so it doesn't know whether it has the proper security credentials
- Terminal doesn't know whether Wi-Fi network provides internet access, so it doesn't know whether to attempt association
- Terminal associates to network, but user's email doesn't work (happens with Web-auth/WISPR when user doesn't launch browser)
- Network selection is just too complicated for non-techie users
  - –E.g., network name (SSID) does not match Venue Name (e.g., *t-mobile* SSID at Starbucks coffee shop)

How does Mobile use 802.11u features to autonomously associate to a hotspot?

- Mobile Wi-Fi radio wakes up periodically and scans
- Mobile actively scans for hotspot and receives:
  - –Internetworking element, identifying AP as 802.11u capable
    - Network Type = chargeable (SPs use this type to identify their hotspots)
    - Internet Access bit set
    - ASRA bit set (indicates AP using Web-auth or supports online sign-up)
  - –Roaming consortium element advertising hotspot owner OUI + top 2 roaming partner's OUIs
- If mobile recognizes OUI, then attempts association using security credentials corresponding to that OUI
  - –Authentication is 802.1x if RSN element received
  - –Authentication is web-auth if no RSN element and ASRA
  - –Note: Each SP must register with IEEE to obtain OUI and OUI must be provisioned into mobile ahead of time

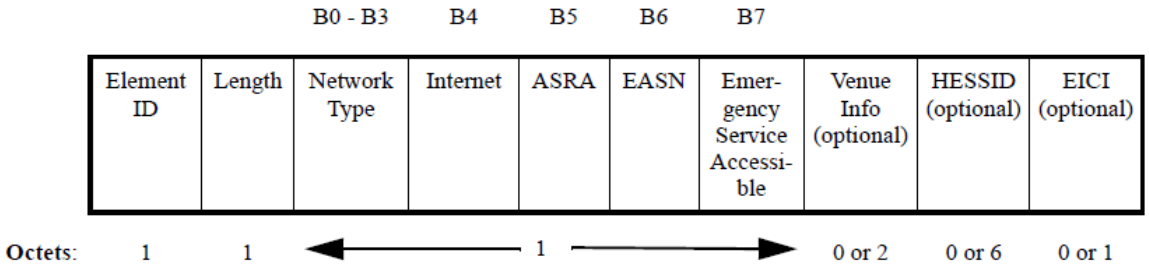
How does Mobile use 802.11u features to autonomously associate to a hotspot (cont.)?

- If mobile recognizes OUI, it attempts association using security credentials corresponding to that OUI
  - –Authentication is 802.1x if RSN element received
  - –Authentication is web-auth if no RSN element and ASRA=1
    - If ASRA=1, mobile transmits native-GAS query to retrieve Network Authentication Type element (authentication details)
- If mobile doesn't recognize OUI, then it transmits a native-GAS query to retrieve:
  - –Roaming consortium list (remainder of OUIs that didn't fit in beacon element)
  - –NAI Realm List
    - Hotspot can accept security credentials for these realms
    - Realms are for hotspot operator or its roaming partners
    - List also provides supported EAP types
    - Notes: enterprises can use this capability for initial provisioning

How does Mobile use 802.11u features to autonomously associate to a hotspot (cont.)?

- If hotspot supports online sign-up (ASRA=1), mobile checks if MSAP supported at hotspot
  - –If so, mobile can sign-up for service (see subsequent slides)
  - –If not, then mobile searches for another hotspot or remains on cellular network
- Note: mobile should include chargeable network type in all active scans so that it will only receive responses from APs set to chargeable network type (at least from 802.11u capable APs)
  - –This conserves mobile's battery energy because it will have far fewer scan responses to stay awake to receive and subsequently process

NDS: Interworking element



- This element is in beacons and probe responses
- Network type:
  - –One of: {*private* | *private with guest access* | *chargeable* | *free*}
  - –STAs can selectively scan for desired network type
- Internet: set to 1 if Wi-Fi network provides internet access
- ASRA (additional authentication step required): set to 1 if Web-auth/WISPR configured
- EASN (EAS notification): set to 1 if EAS message is currently active (uses CAP, common alerting protocol)
- Emergency Service Accessible: set to 1 if emergency services are reachable via the SSID
  - –If network is RSN, then un-authenticated access is provided
  - –May also be an open network

NDS: Roaming Consortium element

Element ID	Length	Number of Native-GAS OUIs	OUI #1	OUI #2 (optional)	OUI #3 (optional)
Octets: 1	1	1	3	3	3

- This element is in beacons and probe responses
- Client scans & receives beacon having this element and can quickly determine if there are any Wi-Fi networks for which it has valid security credentials
- Each SP or consortium of SPs must register with IEEE to obtain OUI
- Element gives OUI for top 3 SPs (or consortium of SPs) having roaming agreements with Wi-Fi access network provider; remainder available via native-GAS query
- Number of Native-GAS OUIs provides number of additional OUIs which will be returned on a native-GAS query (see subsequent slide)

802.11u and TF-Mobility

Thoughts?