

# WLAN as easy as a mobile service

Philipp Michalschik  
LANCOM Systems GmbH

# Mobile Service

- Turn your mobile device on
- Enter PIN to unlock SIM
- Mobile device connects to your service provider automatically

# WLAN

- Turn WLAN on
- Wait for list of scanned SSIDs
- Choose an SSID (that you like)
- Enter credentials (passphrase, username/  
password, web-auth, certificate)

# Network Selection without 802.11u

- Typically: Choice of Connection is up to the user
- Access Type unknown to user (Is this the right SSID for me? Do I have the required credentials? Is Internet available?)
- Different connection options via different SSIDs
- In a hotspot scenario: Each roaming partner requires its own SSID

# 802.11u - Interworking with External Networks

- STA can interwork with external networks (e.g. mobile service provider) in a hotspot or public network
- Information transfer (from external network **prior** to association)
- MAC layer enhancements for end-to-end communication of typically higher layer solutions
- Wi-Fi Alliance (WFA) Certification: Passpoint (based on HotSpot2.0 (HS2.0) element)

# IEEE 802.11u/Passpoint

- STA scans for SSIDs with Interworking and HS2.0 Element
- Access based on credentials on STA rather than just SSID name(s)
- STA can get authenticated by external Authenticator, Hotspot with Proxy AAA service
- One SSID for multiple roaming partners (3GPP, Realm, Roaming partner)
- Initial Connection without user interaction possible, due to already installed credentials (compare to mobile service)

# New Elements in Beacon

- Interworking
- Advertisement Protocol
- Roaming Consortium

▼ Tag: Interworking

Tag Number: Interworking (107)

Tag length: 9

.... 0010 = Access Network Type: Chargeable public network (2)

...0 .... = Internet: 0

..0. .... = ASRA: 0

.0.. .... = ESR: 0

0... .... = UESA: 0

Venue Group: Business (2)

Venue Type: 8

HESSID: WistronN\_11:2d:83 (30:14:4a:11:2d:83)

▼ Tag: Advertisement Protocol

Tag Number: Advertisement Protocol (108)

Tag length: 2

▼ Advertisement Protocol element: ANQP

▼ Advertisement Protocol Tuple: Access Network Query Protocol

.111 1111 = Query Response Length Limit: 127

0... .... = PAME-BI: 0

Advertisement Protocol ID: Access Network Query Protocol (0)

▷ Tag: Roaming Consortium

▷ Tag: Vendor Specific: Wi-FiAll: Hotspot 2.0 Indication



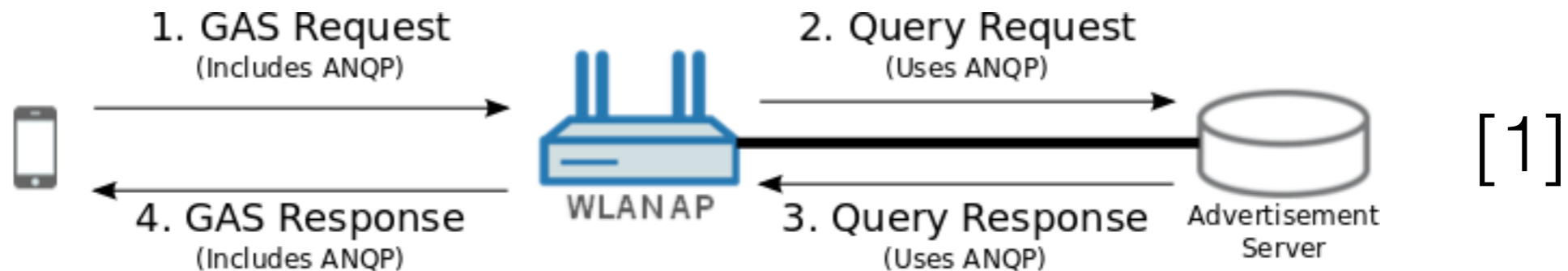
# Interworking Element

- Defines Network Type: Private, Private-GuestAccess, Public(-free/-charge), [...]
- Internet available on SSID?
- Additional Step(s) Required for Access (ASRA): Web-auth/WISPr
- (un-authenticated) Emergency Services Accessible ((U)ESA): USA notifies people e.g. tornado warnings
- Venue Information: Group (Restaurant, Business, Educational, ...); Type (Stadium, Restaurant, Library, ...)
- Homogenous Extended Service Set ID (HESSID): Same „ESS“ across multiple APs (Roaming)

# Roaming Consortium

- Each Service Provider (SP) or group of SPs requires an IEEE organization identifier (OI), globally unique(!)
- Up to 3 OIs in a Beacon (Saves Airtime)
- Additional OIs within Advertisement Protocol

# Advertisement Protocol



- Additional Information to the STA
- General Advertisement Service (GAS) frames to query specific information on device request via ANQP
- Access Network Query Protocol (ANQP)
- STA does not have an IP yet => L2 Protocol

# Advertisement Protocol Cont.

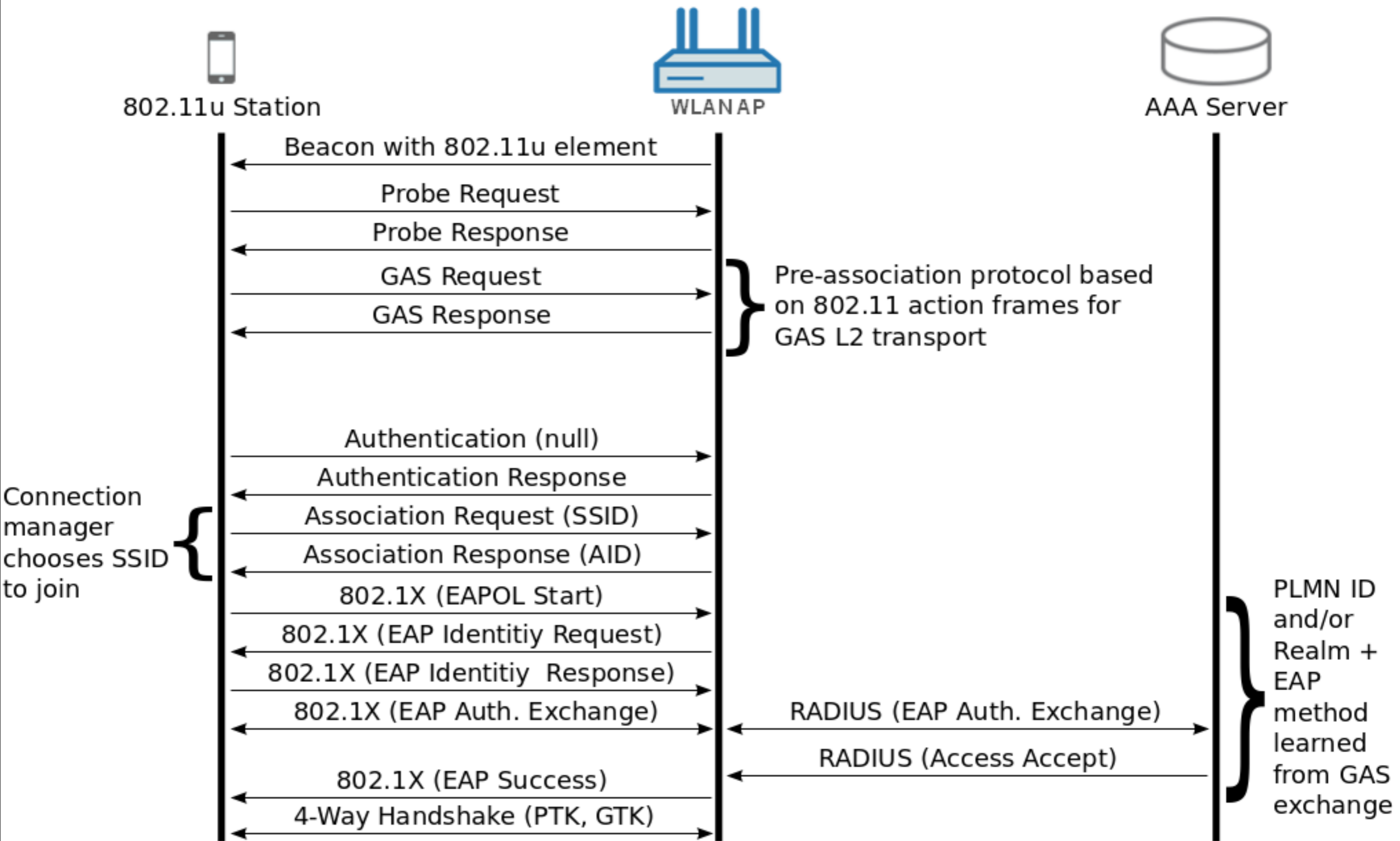
- Venue Name (readable for humans e.g. „Duesseldorf Airport“)
- Network Authentication Type Info:
  - Do users have to accept „Terms and Conditions“?
  - HTTP(S) Redirect URL
  - On-line enrollment
- IPv4 Info: Public IP?, NAT, Port restricted
- IPv6 Info: Available?

# NAI Realm

- Network Access Identifier (NAI): user@realm (e.g. joe@example.com)
- Indicate Extensible Authentication Protocol (EAP) types:
  - Client Credential (Token, certificate, username/password, SIM)
  - Inner authentication method (PAP, CHAP, MSCHAP, MSCHAPv2)

# 3GPP Cellular

- Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC)
- Mobile STA with cellular subscription looks for matching PLMN ID
- EAP-SIM (2G/3G SIM cred.) or EAP-AKA (4G USIM cred.)



# HotSpot2.0

- Vendor specific ANQP format for additional information
- WAN metrics:
  - Link status: up/down/test
  - Down-/Uplink speed, load and load measurement duration
- Connection capabilities: Common IP protocols and ports (Firewall!)
- NAI Home Realm Query: STA asks if AP supports any of its installed/configured NAI realms
- Operating class indication element: On which channels are APs with Passpoint enabled



# Devices

- Passpoint capable devices:
  - Apple iOS 7 devices
  - Android devices (if option is enabled): e.g. Samsung Galaxy S4/Note3, Sony Xperia Z1, LG G2/Flex, HTC One/One Max
  - AP/WLC: Ruckus, Cisco, Aruba, Motorola, Xirrus and LANCOM :-)
- Networks with 802.11u still support non-11u clients

# Conclusion

- Connection decision is moved from the user to the STA (like mobile service)
- Valuable information prior to association
- Slowly but steady growing STA support
- Perfect for mobile data offloading in high density venues (e.g. stadium, shopping malls, airports)

Thank you for your  
attention! Questions?

# Known Issues

- Devices connect to known SSIDs before searching Passpoint SSIDs
- A lot to configure on AP and STA for good connection choices
- Bad Wi-Fi connection is not indicated (You are too far away from the AP)
- WAN connection could be under-provisioned

# Mixed Stuff

- Proper QoS Map (DSCP to UP) Mapping for each Service Provider
- 802.21: Media Independent Handover (MIH) support
- Mobile Data Offloading (MDO) in high density areas e.g. stadium or airport

# Bibliography

[1]: GAS/ANQP graph on page 11: <http://a030f85c1e25003d7609-b98377aee968aad08453374eb1df3398.r40.cf2.rackcdn.com/wp/wp-how-interworking-works.pdf> (page 6)

[2]: Connection graph on page 15: [www.terena.org/activities/tf-mobility/meetings/26/07-11u-Dave.pptx](http://www.terena.org/activities/tf-mobility/meetings/26/07-11u-Dave.pptx) (page 9)