IEEE 802 Enhanced Network Detection and Selection

Date: 2013-08-26

Authors:

Name	Affiliation	Phone	Email
Max Riegel	NSN	+49 173 293 8240	maximilian.riegel@nsn.com

Abstract

The presentation introduces enhanced requirements for IEEE 802 access network detection and selection aligned to recent work in IEEE 802.11 and Wi-Fi Alliance on public Wi-Fi access (Hotspot 2.0).
IEEE 802.11u introduced an Access Network Query Protocol (ANQP), which supports more comprehensive network selection functionalities and builds the base for the Hotspot 2.0 access procedures, which might be well suited for deployments of other IEEE 802 access technologies.

IEEE 802 Enhanced Network Detection and Selection

(OmniRAN Gap Analysis)

Max Riegel

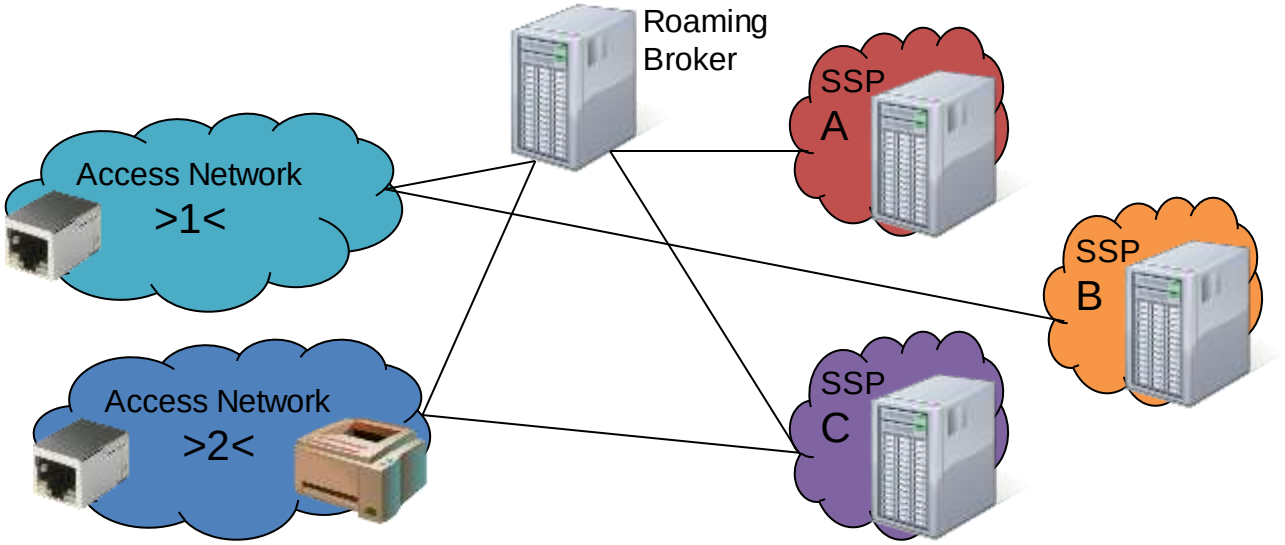
NSN

ToC

- The Access Network Selection Challenge
- The IEEE 802.11 approach
  - ANQP Usage by Hotspot 2.0
  - E.g. ANQP Information Elements
  - Upcoming Hotspot 2.0 Functionalities
- ANQP would fit into any IEEE 802 technology
- IEEE 802.1X-2010 Network Announcements
  - Access Information per NID
- Conclusion

The Access Network Selection Challenge

- Challenges in access network selection occur with
  - Multiple different access networks
  - Multiple subscriptions
  - Specific service requirements
  - No a-priori knowledge about offered services



SSP = Subscription Service Provider

The IEEE 802.11 Approach

- A Wi-Fi terminal scans the air for finding the near-by access points
  - Either by passive scanning (Beacon)
  - or by active scanning (Probe Request & Probe Response)
- Questions arising when discovering an access point:

Is this my Home Service Provider?

Is this a Visited Service Provider?

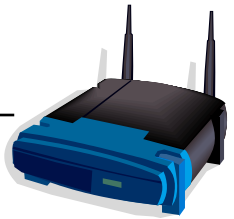
Will this Service Provider support the service I am looking for?

Do I need any special provisioning for this Service Provider?

?

- The information in the beacon or probe response is often not sufficient to make the appropriate decision
- IEEE802.11u defines a protocol allowing to query additional information about the Wi-Fi access before initiating the association and authentication
- GAS (Generic Advertisement Service) provides a container for the ANQP (Access Network Query Protocol), which provides more information about the Wi-Fi access

ANQP Usage by Hotspot 2.0



Hotspot 2.0 capable AP Beacons and Probe Response

RSN IE(WPA2), Interworking Element (includes HESSID and Venue Information), Advertisement Protocol Element (Indicates ANQP), Roaming Consortium Element(A list of roaming consortium identifier), The Hotspot 2.0 Indication element

- Hotspot 2.0 capable STAs scan for networks and discover an AP advertising Hotspot 2.0 capability.
- Hotspot 2.0 capable STA uses ANQP to the AP to determine properties of the Hotspot 2.0 Access Network. The Hotspot capable STA selects the ANQP query elements it requires to query the Hotspot 2.0 network for Interworking Service information.

GAS Initial Request Frame(Advertisement Protocol = ANQP;

ANQP Query = {Venue Name, Network Auth, Roaming Consortium, IP Address Type, NAI Realm, 3GPP Cellular information, Domain Name; Operator Friendly Name, WAN Metrics, Connection Capability}

GAS Initial Response Frame(Advertisement Protocol = ANQP;

(Venue Name; Network Auth; Roaming Consortium; IP Address Type; NAI Realm; 3GPP Cellular information; Domain Name; Operator Friendly Name,; WAN Metrics; Connection Capability)

- Hotspot 2.0 capable STA evaluates the response based on its Hotspot 2.0 subscription information and associated policy and choose to associate to the AP.

Associate and WPA2 EAP Authentication

Secure WPA2 Data Connectivity

E.g. ANQP Information Elements

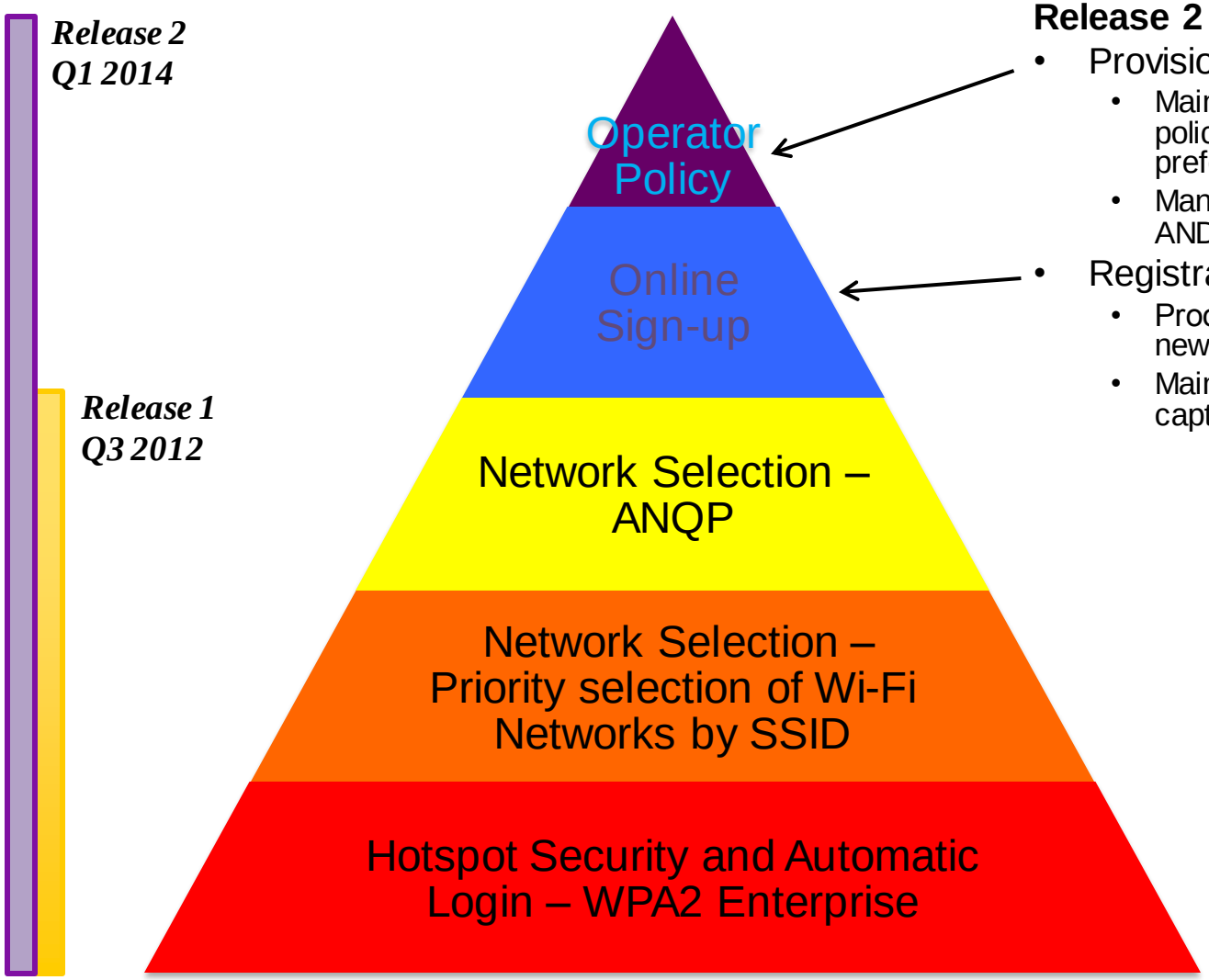
IEEE 802.11 ANQP Information Elements

- Venue Name
  - Provides zero or more venue names associated with the BSS to support the user's selection.
- Network Authentication Type
  - Provides a list of authentication types carrying additional information like support for online enrollment or redirection URL.
- Roaming Consortium
  - Provides a list of information about the Roaming Consortium and/or SSPs whose networks are accessible via this AP.
- IP Address Type Availability
  - Provides STA with the information about the availability of IP address version and type that could be allocated to the STA after successful association.
- NAI Realm
  - Provides a list of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via this AP; optionally amended by the list of EAP Method, which are supported by the SSPs.
- 3GPP Cellular Network
  - Contains cellular information such as network advertisement information e.g., network codes and country codes to assist a 3GPP non-AP STA in selecting an AP to access 3GPP networks.
- Domain Name
  - Provides a list of one or more domain names of the entity operating the IEEE 802.11 access network.

Hotspot 2.0 ANQP Information Elements

- HS Query list
  - Provides a list of identifiers of HS 2.0 ANQP elements for which the requesting mobile device is querying in a HS ANQP Query.
- HS Capability list
  - Provides a list of information/ capabilities that has been configured on an AP. The HS Capability list element is returned in response to a GAS Query Request.
- Operator Friendly Name
  - Zero or more operator names operating the IEEE 802.11 AN.
- WAN Metrics
  - Information about the WAN link connecting a IEEE 802.11 AN and the Internet.
- Connection Capability
  - Provides connection status of the most commonly used communications protocols and ports.
- NAI Home Realm Query
  - Used by the STA to determine if the NAI realms for which it has security credentials are realms corresponding to SPs or other entities whose networks or services are accessible via this BSS
- Operating Class Indication
  - Provides information on the groups of channels in the frequency band(s) the Wi-Fi access network is using

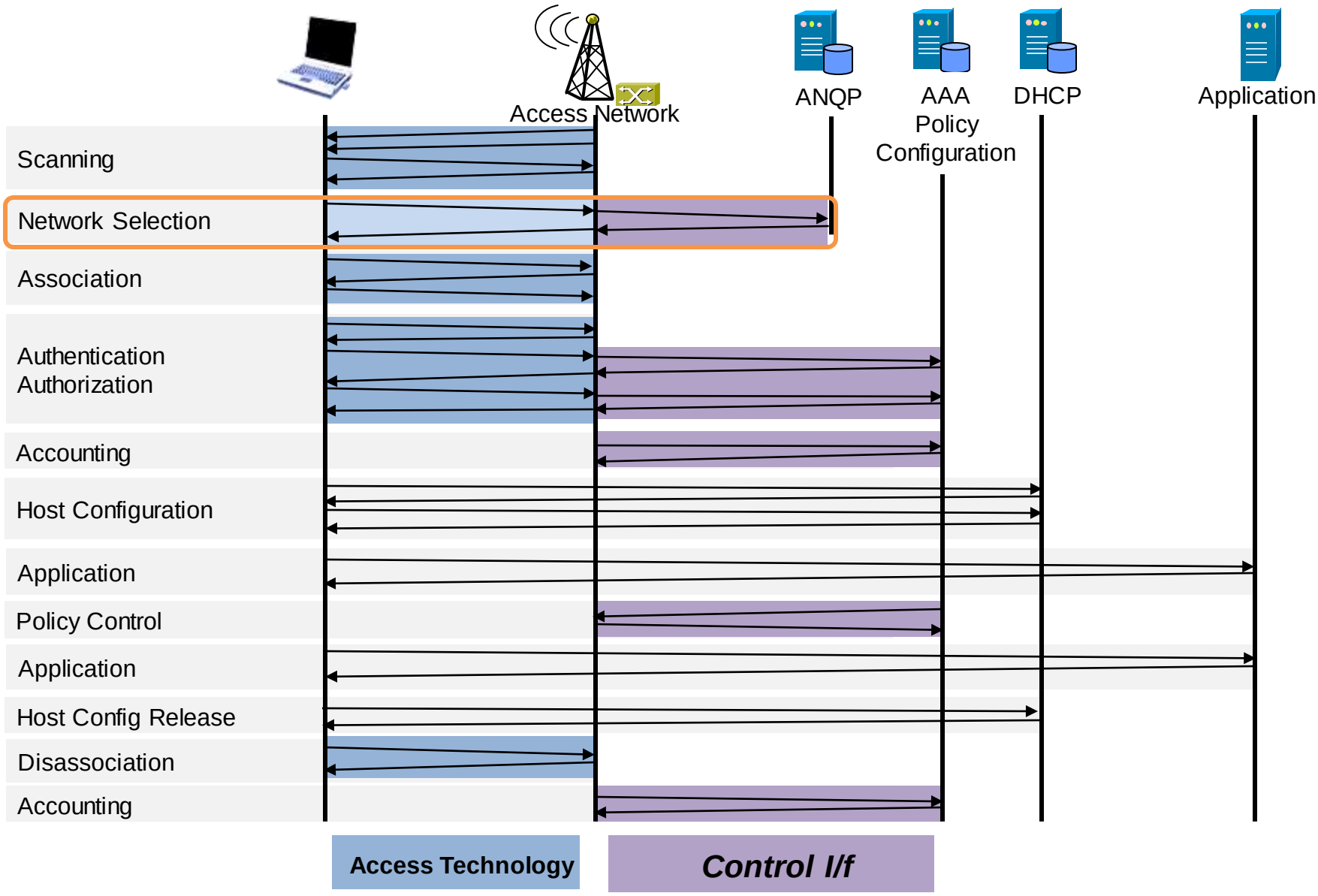
Upcoming Hotspot 2.0 Release 2 adds powerful functions for IEEE 802 access networks



Release 2 adds to Release 1:

- Provisioning
  - Mainly provisioning of operator policies for automatic selection of preferred Wi-Fi access networks
  - Management Object different to ANDSF
- Registration
  - Procedure to establish 'online' a new subscription
  - Mainly replacement of the legacy captive portal

ANQP would fit into any IEEE 802 technology



Network Announcements provided by IEEE 802.1X-2010

- What network(s) or network service(s) are available
- Is access to that network already available, or is authentication or secured connectivity required
- What authentication and secure connectivity mechanisms are required or available
- What credentials should be presented if EAP is to be used
- What cached CAKs can be used with a reasonable chance of success
- What level of access (authorization) is or may be provided

TLV type	TLV name	Set	Validity[a]	Version 3[b]	Reference
0–110	Individual TLVs reserved for future standardization	No	Reserved for future standardization.	—	
111	Access Information	No	Announcement, Announcement-Req, EAPOL-Start: Global, NID Set	M	11.12.2
112	MACsec Cipher Suites	No	Announcement: Global, NID Set	M	11.12.3
113	Key Management Domain	No	Announcement: Global, NID Set	M	11.12.5
114	NID (Network Identifier)	NID Set	Announcement, Announcement-Req, EAPOL-Start	M	11.12.1
115–125	Set TLVs reserved for future standardization.	Yes	To be specified	—	
126	Organizationally Specific Set TLV	Yes	Specified by administering organization	O	11.12.5
127	Organizationally Specific TLVs	No		O	11.12.5

Access Information per NID

Information	Field	Indicates
Access Status	Octet 1: bits 1 (l.s.b) - 2	No Access (0); Remedial Access (1); Restricted Access (2); Expected Access (3)
Access Requested	Octet 1: bit 3	Set if access requested for this NID
Unauthenticated Access	Octet 1: bits 4 - 5	No Access (0); Fallback Access (1); Limited Access (2); Open Access (3)
Virtual Port Access	Octet 1: bit 6	Set if access can be provided by a virtual port.
Group Access	Octet 1: bit 7	Set if access can be through a Group CA
Reserved	Octet 1: bit 8	Reserved for future standardization. Encode as zero.
Access Capabilities	Octet 2: bit 1 (l.s.b)	EAP
	Octet 2: bit 2	EAP + MKA
	Octet 2: bit 3	EAP + MKA + MACsec
	Octet 2: bit 4	MKA
	Octet 2: bit 5	MKA + MACsec
	Octet 2: bit 6	Higher Layer (WebAuth)
	Octet 2: bit 7	Higher Layer Fallback (Webauth)
	Octet 2: bit 8 (m.s.b)	Vendor specific

Conclusion

- Network Announcements according to IEEE 802.1X-2010 provide basic information for network detection and selection
  - However missing capabilities to serve more complex access network scenarios
- IEEE 802.11u introduced by ANQP a query/response protocol to handle even very complex scenarios
  - Supporting complex roaming scenarios with roaming brokers
  - Allowing for pre-authentication service discovery
  - Enabling powerful Hotspot 2.0 access procedures

- It seems to be desirable to consider implementation of ANQP within other IEEE 802 access technologies, e.g. IEEE 802.3
  - Potentially allowing to deploy enhanced Hotspot 2.0 procedures like provisioning or on-line sign-up also on wired Ethernet