Review of draft-adrangi-eap-network-discovery-05 for IEEE 802.1AE/af

Paul Congdon
IEEE 802 Plenary
San Antonio, Tx
November 2004
EAP Network Discovery

- Usage scenarios
- Relevance to 802.1af
- Review of draft-adrangi-eap-network-discovery-05
Usage Scenarios – Wired Hotspots

• Imagine:
  – Wired ports where multiple service providers can deliver service simultaneously
  – Wired customers who have credentials with multiple service providers
  – Public or uncontrolled environments where it is difficult to enforce what is attached to the wire.
  – Wired network services are selected similar to how wireless network SSIDs are chosen today.
802.3 Hotspot

Metropolitan Area Service Provider

Red Provider AAA Server

Blue Provider AAA Server

Hotspot

unmanaged shared media concentration

Closet

wall jack
Possible scenario with AE/af

1. Select Network Access Identity (NAI) for network service of choice
2. Authenticate using 802.1X & EAP
3. Provision master key for 802.1AE via EAP
4. Establish CA using KSP
5. Maintain CA using KSP
• Provides identity selection hints to an EAP peer (aka client)
• Peer chooses most appropriate NAI for EAP-Identity/Response
• EAP-Identity/Request contains a list of identity hints (NAI Realms)
• List of realms is after a displayable string and NULL character
• Example EAP-Identity/Request:

  01                        ; Code: Request
  00                        ; Identifier: 0
  00 43                     ; Length: 67 octets
  01                        ; Type: Identity
  48 65 6c 6f 21 00 4e      ; "Hello\0NAIRealms=example.com;mnc014.
  41 49 52 65 61 6c 6d 73   ; mcc310.3gppnetwork.org"
Authenticator Originated

1. EAP Identity/Request (NAIRealms) <------------------
2. EAP Identity/Response------------------>
   <-------------------EAP conversation---------------------->
Server Originated

EAP Peer | Authenticator | local RADIUS proxy/server | home RADIUS server
---|---|---|---

1. Access-Request (EAP-Start)

2. Access-Challenge (EAP Identity/Request with NAIRealms)

3. EAP Identity/Request (NAIRealms)

4. EAP Identity/Response

5. Access-Request (EAP Identity/Response)

6. Access-Request (EAP Identity Response)

EAP conversation
Server Originated (option 2)

1. EAP Identity Request (w/o NAIRealms)
   <------------------------------------------------->
2. EAP Identity Response

3. Access-Request (EAP Identity Response)
   <------------------------->
4. Access-Challenge (EAP Identity Request with NAIRealms)
   <------------------------->
5. EAP Identity Request (NAIRealms)
6. EAP Identity Response
   <------------------------->
7. Access-Request (EAP Identity Response)

8. Access-Request (EAP Identity Response)

EAP conversation
ID status

• Document is currently in WG last call
  – Closes Nov 22\textsuperscript{nd}
  – Still available for 802.1 comments
• Document is a dependency on 3GPP standards
• Reviewed by 802.11 (WIEN) and deemed acceptable, however they will proceed with changes to MAC control frames as well.