Radius Extensions for Key Management in WLAN Network

Li Xue

Dacheng Zhang

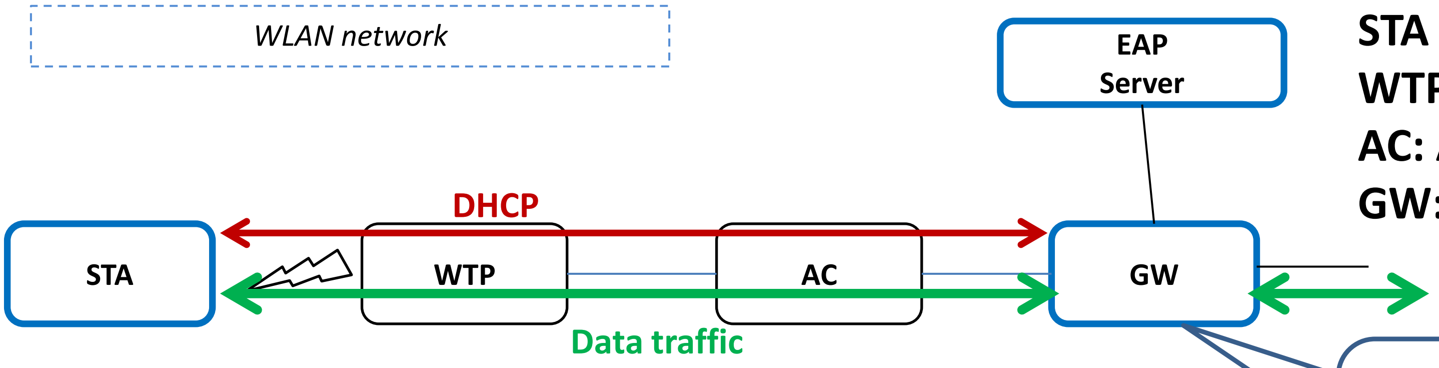
Bo Gao

IETF #89

Background

- This work has been presented in IETF 87.
- It was criticized that the motivation scenario is not very strong.
- We realized that the discussion on this issue is also made in BBF. The feedback is positive.

Motivation Scenario (1)

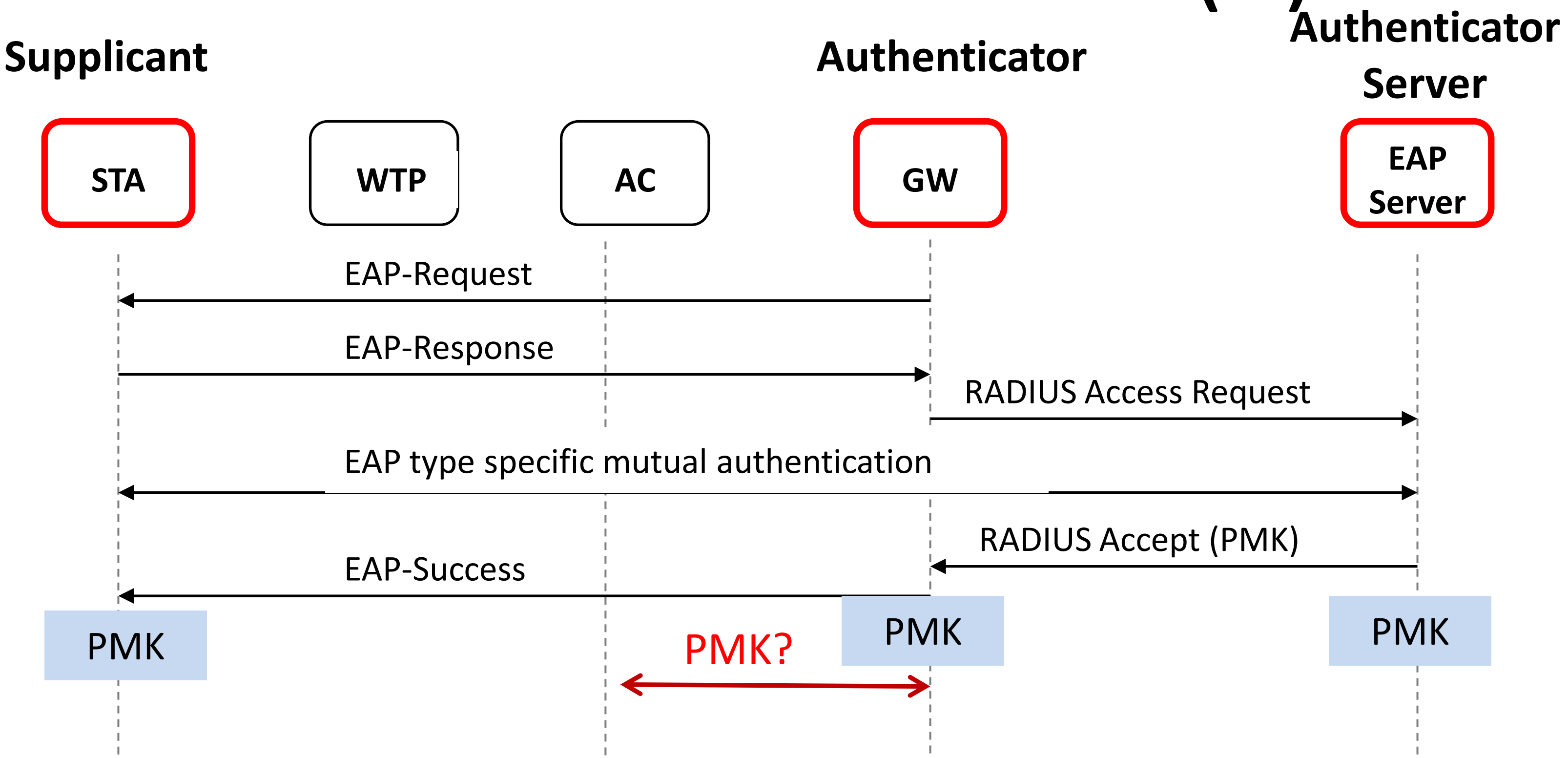


STA (UE): Mobile Device
WTP: AP
AC: Access Controller
GW: Gateway

IP address Assignment
Charging
QoS

- In a WLAN network, GW is responsible for:
  - ✓ Authentication and Authorization
  - ✓ IP address assignment for the authenticated STA
  - ✓ Charging, QoS enforcement etc
- GW has to know the authentication result of a STA to perform its subsequent operations (e.g., IP address assignment, charging), which is a good reason to deploy Authenticator on the GW.

Motivation Scenario (2)

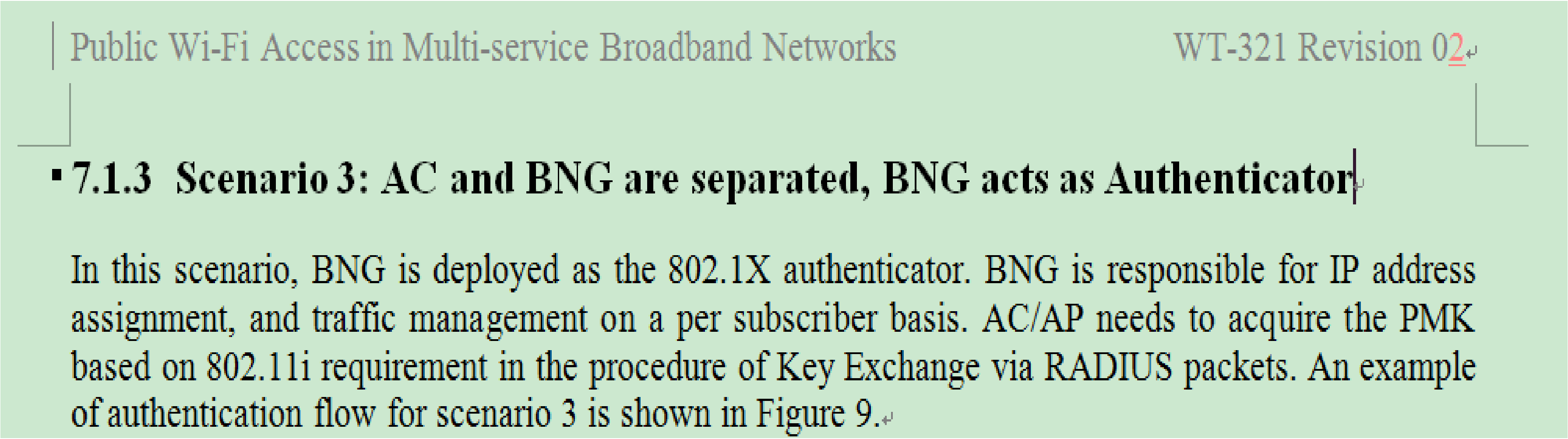


In a WLAN network, when a STA tries to connect to the WTP, mutual authentication with a EAP server is needed.

- PMK (Pairwise Master Key) is generated and distributed to the **STA** and the **Authenticator (GW);**
- Because PMK is used for securing the subsequent communication between the STA and the WTP, it needs to be forwarded from the **GW** to **WTP/AC**.

Motivation Scenario (3)

- This motivation scenario is already discussed and supported by multiple operators in SDO- BBF (Broadband Forum) WT-321 (Public Wi-Fi Access in Multi-service Broadband Networks) http://www.broadband-forum.org
- Because the gap in this motivation scenario came from the operators deployment requirements, a standard solution is desired for interoperation, rather than private extensions.

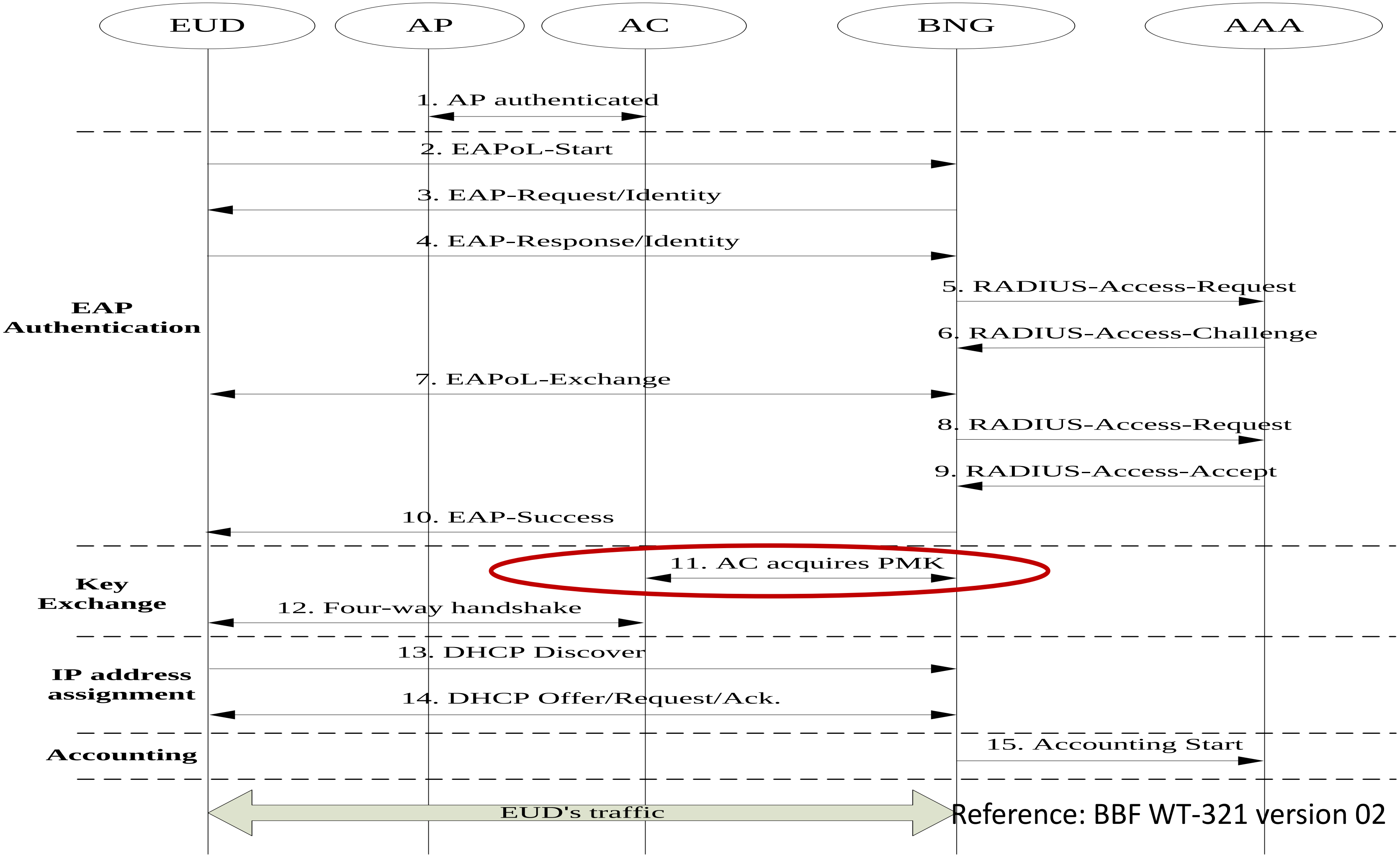


Public Wi-Fi Access in Multi-service Broadband Networks WT-321 Revision 02

7.1.3 Scenario 3: AC and BNG are separated, BNG acts as Authenticator

In this scenario, BNG is deployed as the 802.1X authenticator. BNG is responsible for IP address assignment, and traffic management on a per subscriber basis. AC/AP needs to acquire the PMK based on 802.11i requirement in the procedure of Key Exchange via RADIUS packets. An example of authentication flow for scenario 3 is shown in Figure 9.

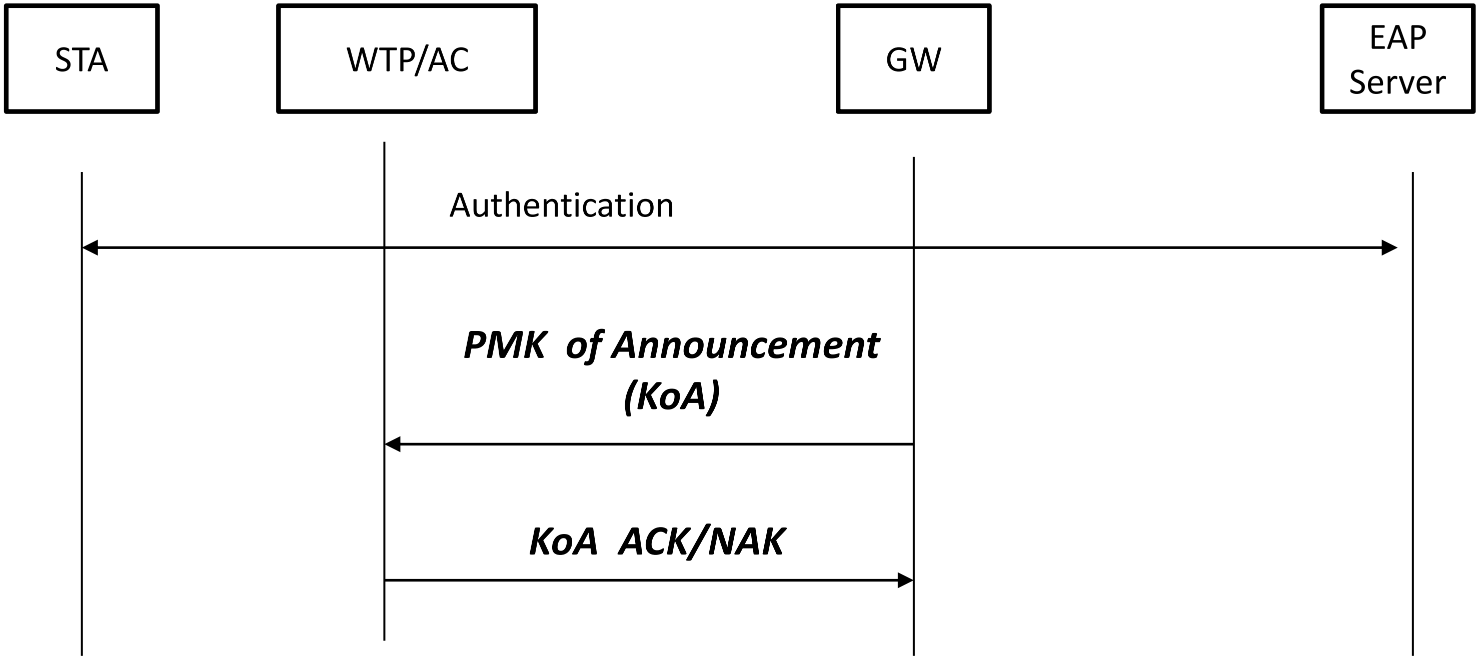
Motivation Scenario (3) cont’



Reference: BBF WT-321 version 02

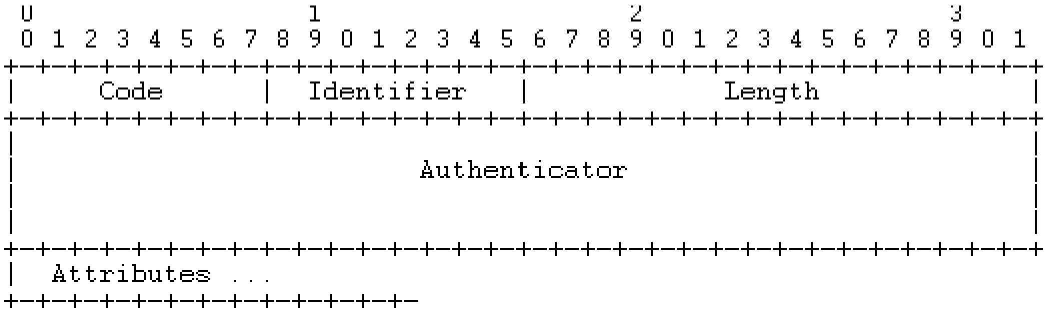
Our Solution

- Control messages used for PMK transported from GW to AC is defined.



● **Radius packets , KoA, KoA ACK/NAK , are extended to support Key Management**

Packet Format



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                         Authenticator                         |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Code:
  - 100: PMK of Announcement (KoA)
  - T01: KoA ACK
  - T02: KoA NAK
- Attributes:
  - Calling-Station-Id: It is used to bind the PMK to a special STA. The call-station-id attribute may be included within KoA, KoA-ACK/NAK messages.
  - ***Keying-Material (New)***
  - ***KoA Feedback (New)***

Feedback

- Can this work be adopted as a WG draft?

Thank you