Radius Extensions for Key Management in WLAN Network

Li Xue

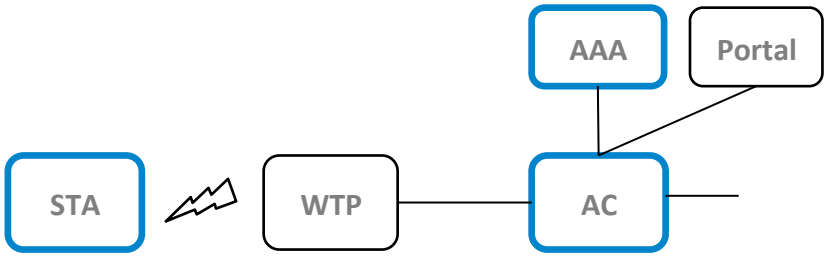
Bo Gao

Introduction

- Analyze the scenario and requirement
- Problem Statement for key management that have arisen so far during STA authentication process in WLAN network.
- Describe the solution based on RADIUS extension.

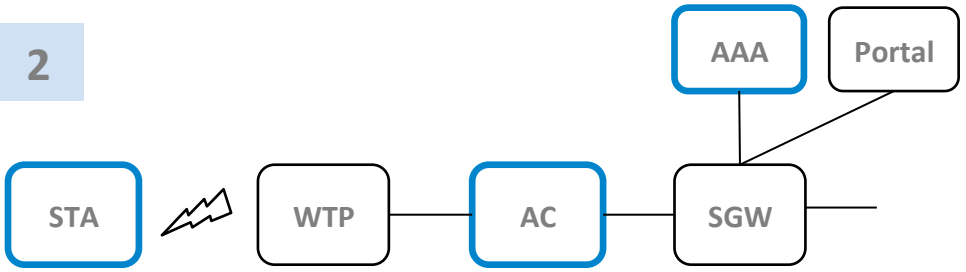
Public WLAN Network Scenarios Overview

1



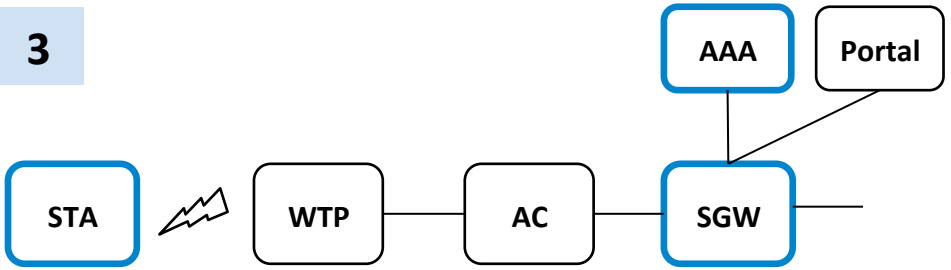
1. AC is converged the function of SGW.
   - ✓ In EAP authentication architecture, AC acts as the Authenticator, AC is responsible for STA IP assignment.
   - ✓ **It is out the scope of the document.**

2



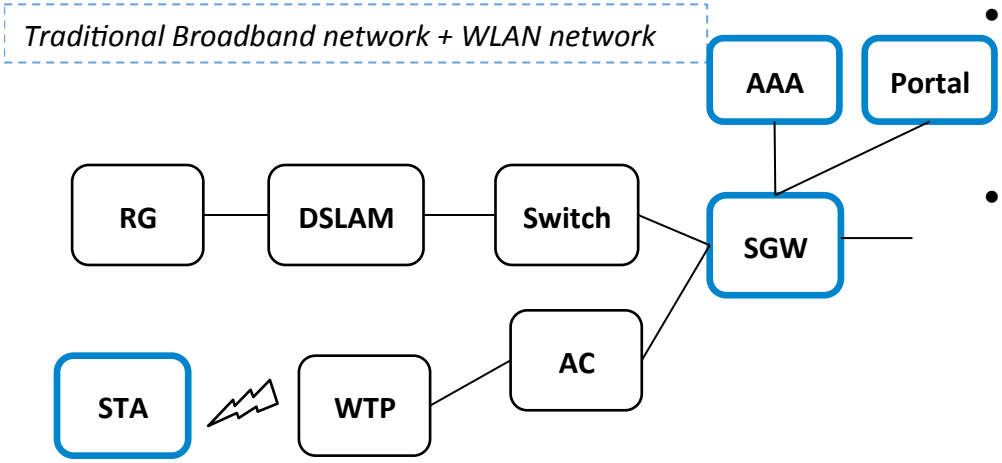
2. AC and SGW is separated.
   - ✓ In EAP authentication framework, AC acts as the Authenticator, SGW is responsible for STA IP assignment.
   - ✓ **It is out the scope of the document.**

3



3. AC and SGW is separated.
   - ✓ In EAP authentication framework, SGW acts as the Authenticator.
   - ✓ In this scenario, AC needs to acquire the PMK information.

Illustration: Traditional Operator WLAN Network Characters



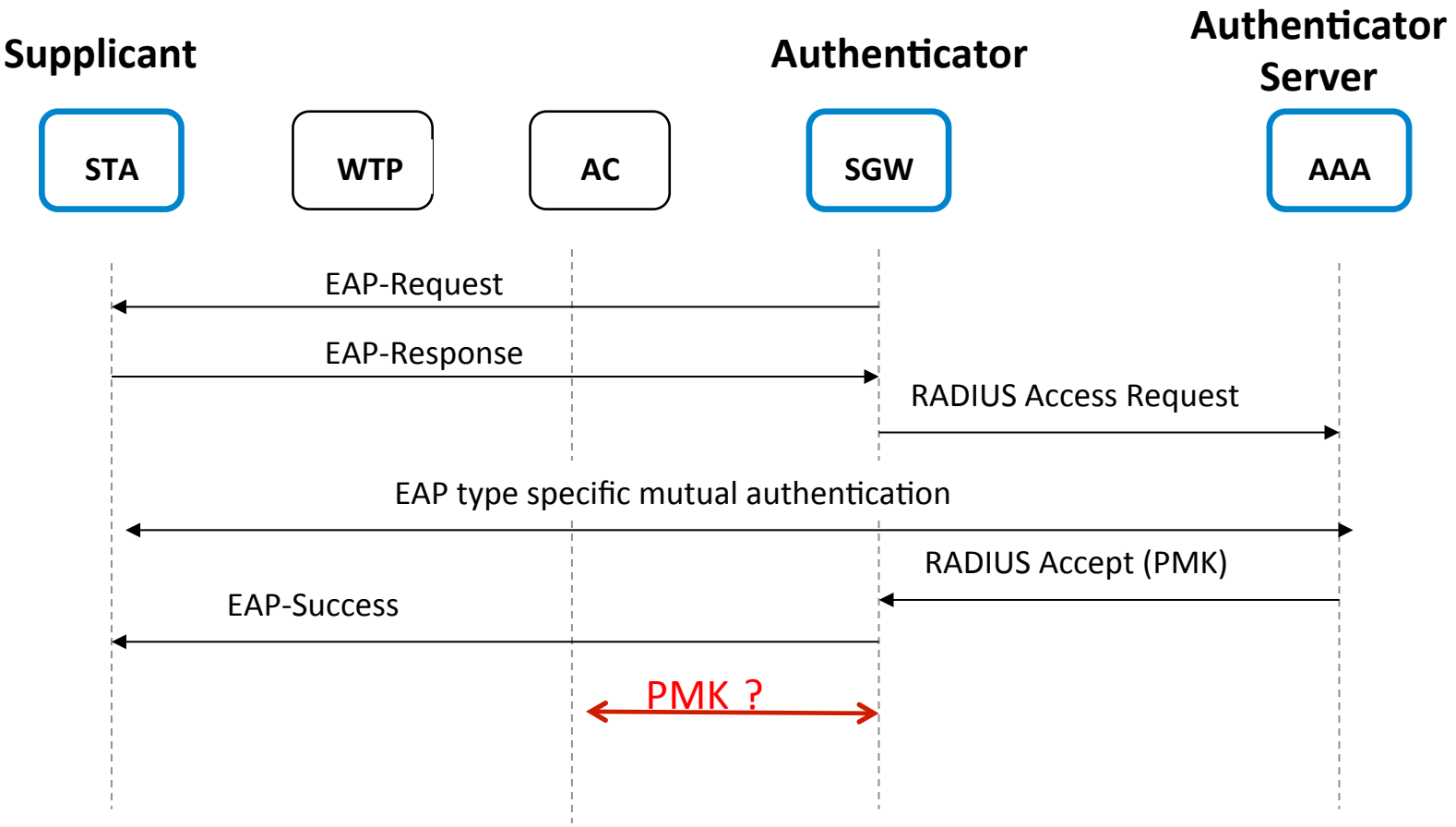
Function	AC acts as Authenticator		SGW acts as Authenticator	
	AC	SGW	AC	SGW
EAP Authenticator	X			X
EAP Authentication proxy		X		-
Portal Proxy		X		X
User Management		X		X
IP assignment		X		X

- WLAN network is one access technology which is added to previous broadband network.
- SGW is responsible for:
  - ✓ the service gateway for Broadband service, responsible for authentication.
  - ✓ STA IP address assignment
  - ✓ User management, for example, charging, etc.
  - ✓ Portal Authentication for WLAN.
  - ✓ EAP Authenticator for Mobile devices.

The reasons for SGW acting as Authenticator

- User Management requirements
  - ✓SGW needs to achieve user management based on user information, via EAP Authenticator or EAP authentication proxy
  - ✓ SGW needs to achieve charging based on user information, via EAP Authenticator or EAP authentication proxy
- Network Operation & Maintenance requirements
  - ✓ SGW is deployed more centralized than AC to reduce the AAA overloading communications
- Advantages
  - ✓ The operator can deploy simple AC plus SGW as uniform authentication function with low OPEX
  - ✓The network and devices can be managed with low CAPEX

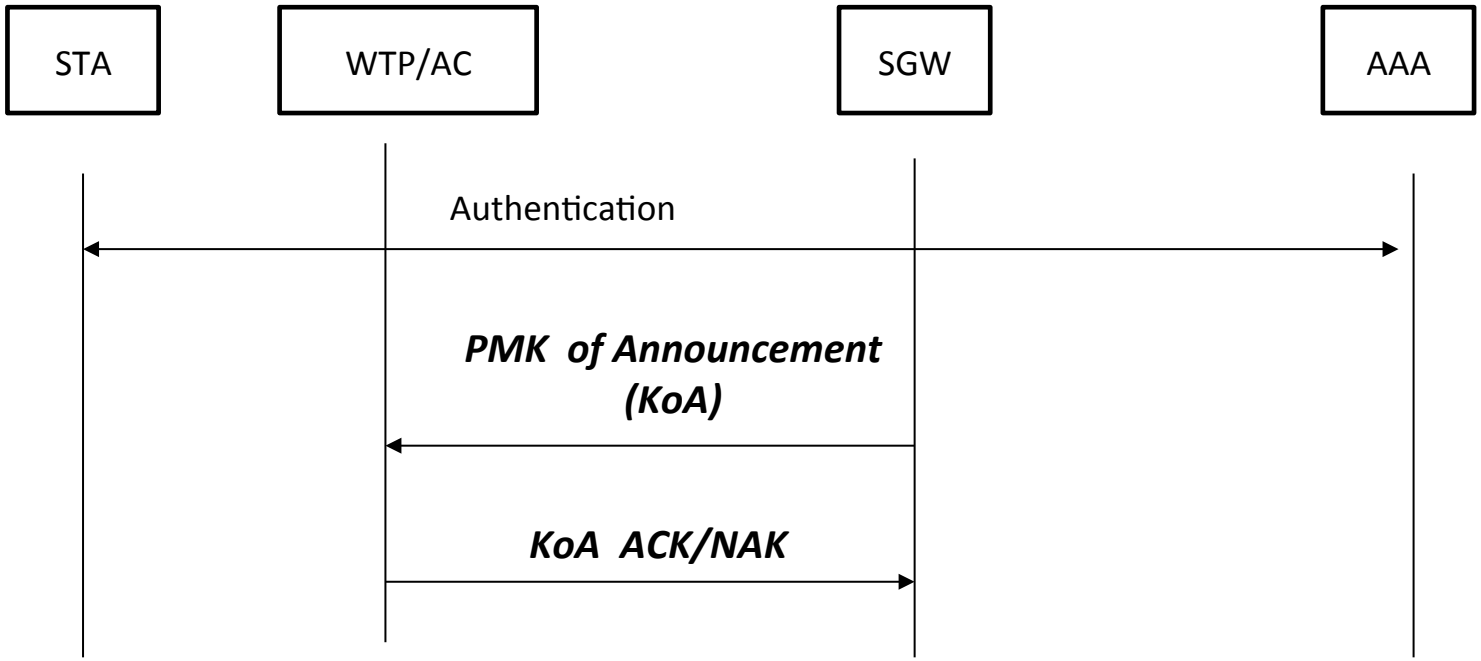
Problem Statement



- If the authenticator function is deployed on SGW node, there is an issue to achieve traffic encryption/decryption between STA and WTP/AC.

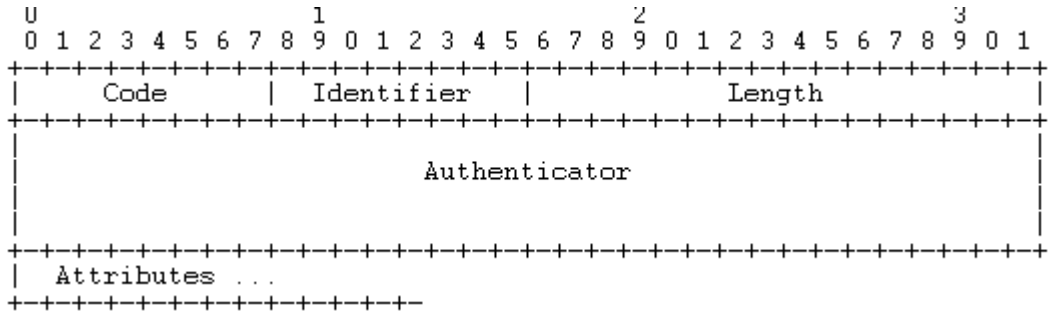
Solution Procedure

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



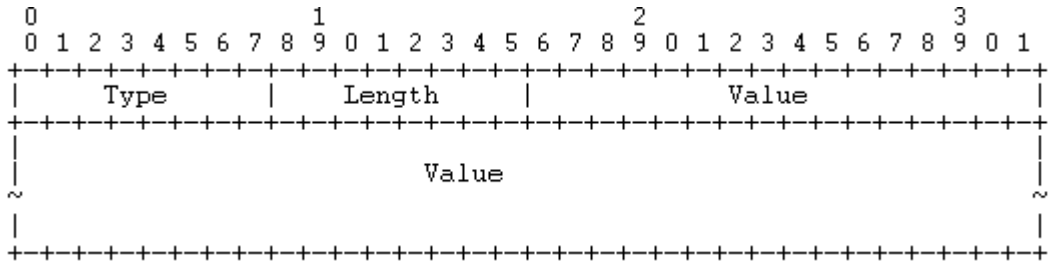
- **Radius packets , KoA, KoA ACK/NAK , are extended to support Key Management**

Packet Format



- Code:
  - TBD: PMK of Announcement (KoA)
  - TBD: KoA ACK
  - TBD: KoA NAK (optional)
- 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)***

New Attributes



- Keying-Material
  - This attribute is included in KoA, and KoA ACK/NAK messages
  - Type: TBD
  - Value: PMK (32 Octets)
- KoA-Feedback
  - This attribute is included in KoA ACK/NAK messages
  - Type: TBD
  - Value: 2 Octets, containing the feedback from the AC when received the KoA message. Following values are suggested：
    - 0: Succeed
    - 1-8: Rejected

Next Step

- Security consideration
  - Clarify the security mechanism for key-management announcement
  - Security mechanisms
    - IP Sec
    - Radius MD5
    - Other?

Thank you

Backup: The Procedure for AC acts as Authenticator, SGW supports Radius-Proxy