Key Management for Link Layer Security

Kwangjo Kim*, Hyunrok Lee*,
Taehwan Yoo, Jeesook Eun****

Information and Communications University (ICU) *
Electronics and Telecommunications Research Institute (ETRI) **

Content

- 802.11i overview
- Proposed Key management
- Authentication
- Mobility
- Ensuring mobility

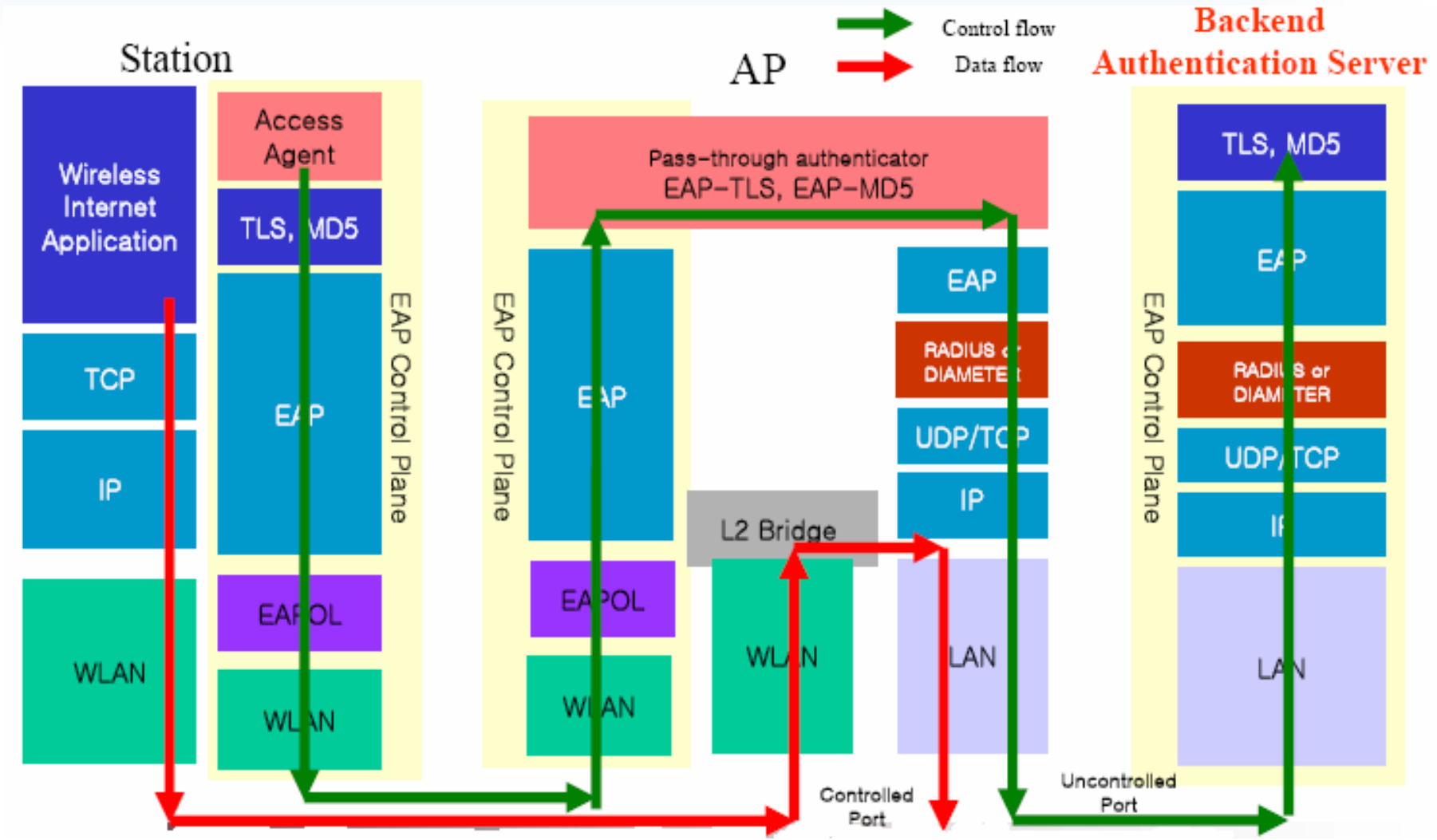
802.11i - Overview (1/2)

- **Confirmed Standard - 2004.6.24**
- **Data Security (Key Management/Crypto Algorithm)**
  - IEEE 802.1aa
    - Accept 802.11i Key Descriptor
    - Define Key exchange state machine
  - IEEE 802.11i
    - RSN (Robust Security Network)
    - Access control based on 802.1X
    - Dynamic Key Exchange and Management
    - New Crypto Algorithm
      - TKIP – For backward compatibility (WEP)
      - CCMP – AES-CCM mode

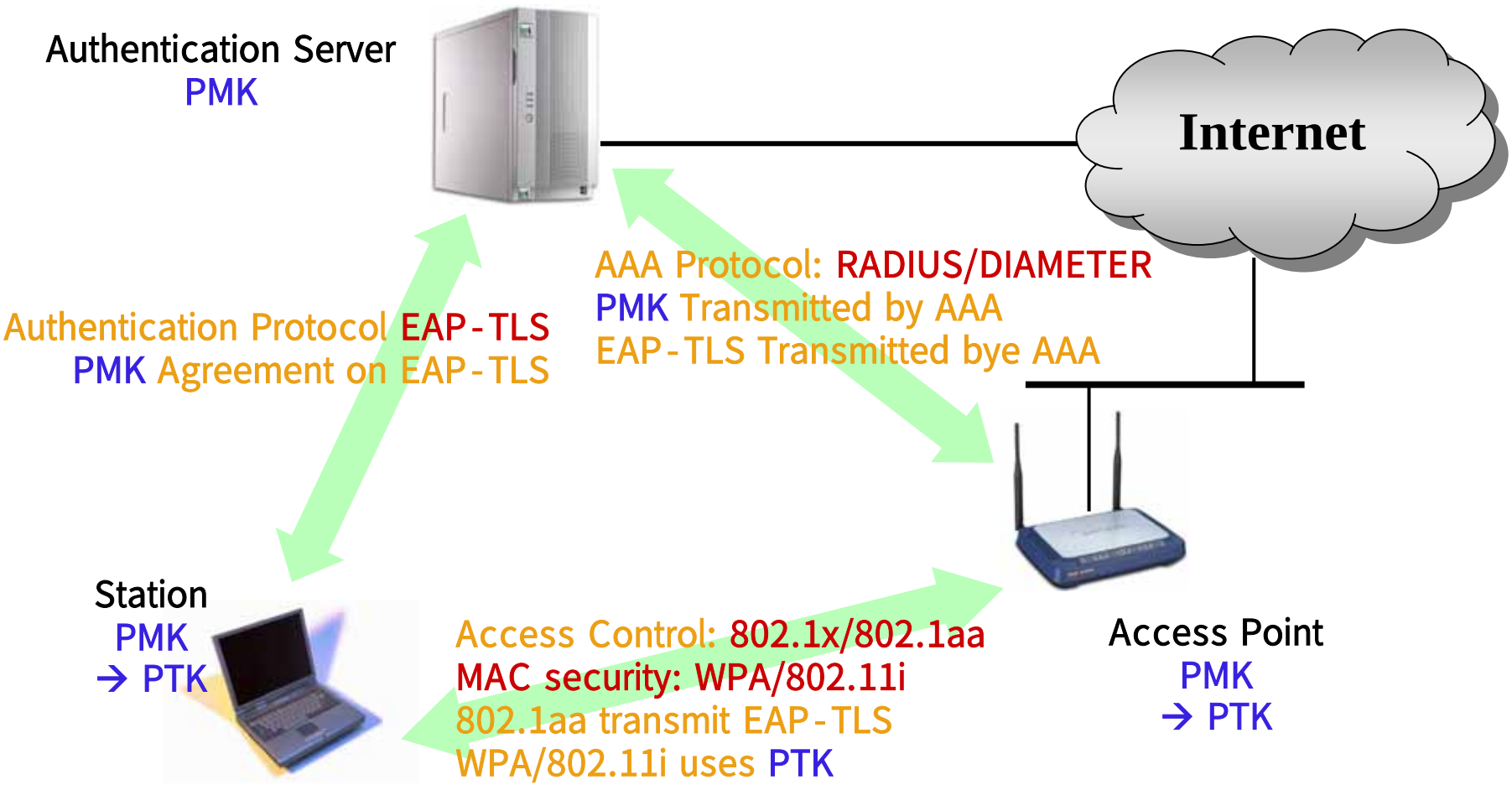
802.11i - Overview (2/2)

- **User Authentication**
  - IEEE 802.1X
    - Port-Based Network Access Control
    - Before authentication: uncontrolled port
      After authentication: controlled port open
  - IEEE 802.1aa
    - Extra document for 802.1X
    - After authentication and Key exchange: controlled port open
  - EAP (Extensible Authentication Protocol)
    - Various authentication mechanism will be acceptable
    - EAP-MD5, EAP-TLS, EAP-TTLS
  - AAA (Authentication, Authorization and Accounting) Server
    - RADIUS (Remote Authentication Dial In User Service) Server
      - RFC 2865
    - Diameter Server
      - RFC 3588

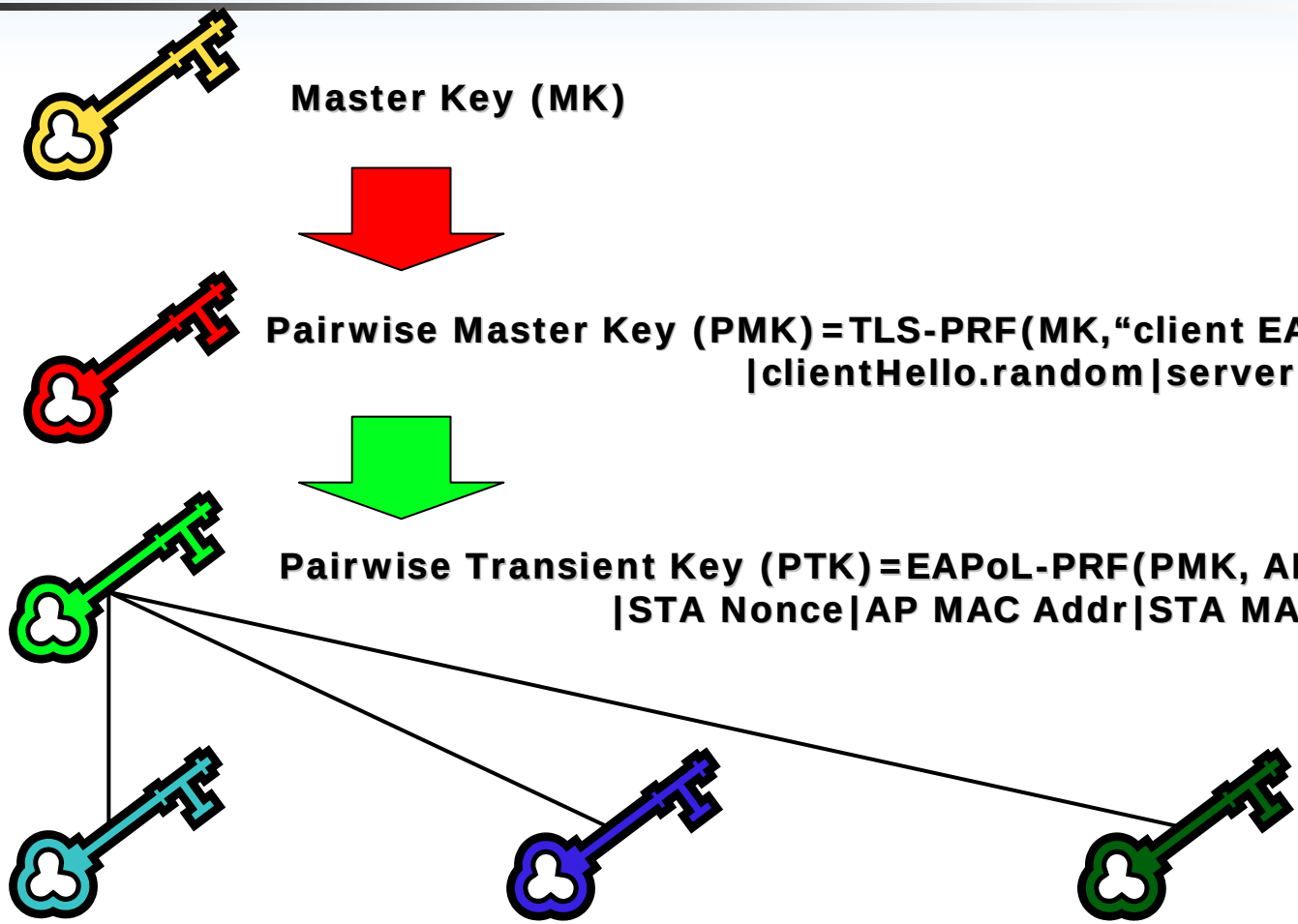
IEEE 802.11i - Authentication



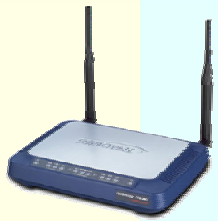
IEEE 802.11i - Authentication & Key Exchange



802.11i - Pairwise Key Hierarchy



802.11i – Key Management



Step1: Use RADIUS to push PMK from AS to AP

Step2: Use PMK and 4-way Handshake
to derive, bind, and verify PTK

Step 3: Use Group Key Handshake
to send GTK from AP to STA

Proposed Key Management

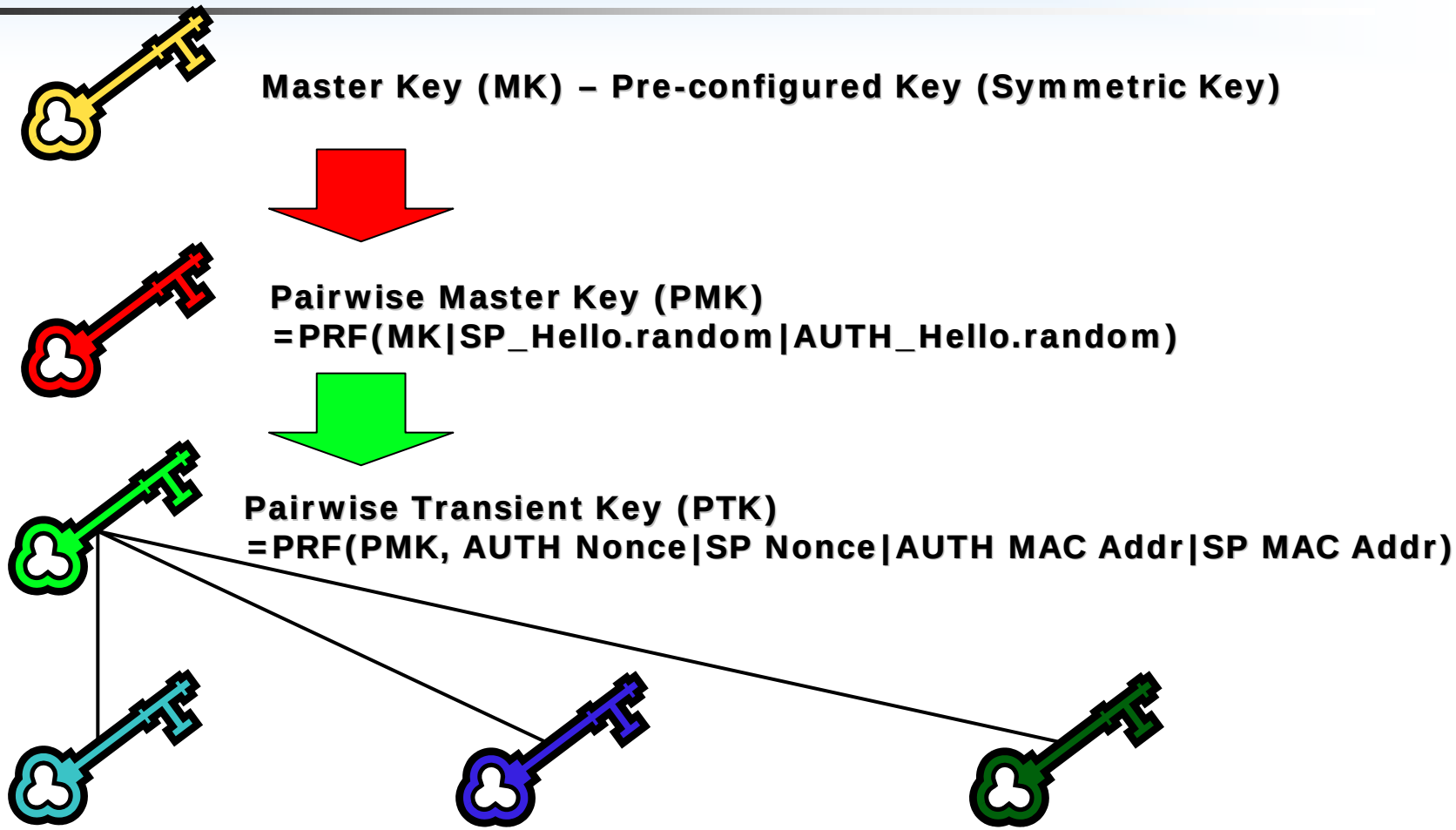
- DISCOVERY
- Key Hierarchy
- Key Exchange with verification

DISCOVERY

- **Cannot avoid this process!!**
- **Following factors should be configured before operation.**
  - Is there any valid MACsec module?
  - Where is Cryptography function?
    - Tx only? Rx only? Both possible?
  - What is Cryptography algorithm?
    - GCM-AES-128,CCM-AES-128,OCB-AES-128,RSA?
  - What is Key distribution algorithm?
    - Diffie-Hellman?
  - And so on…

Key Hierarchy

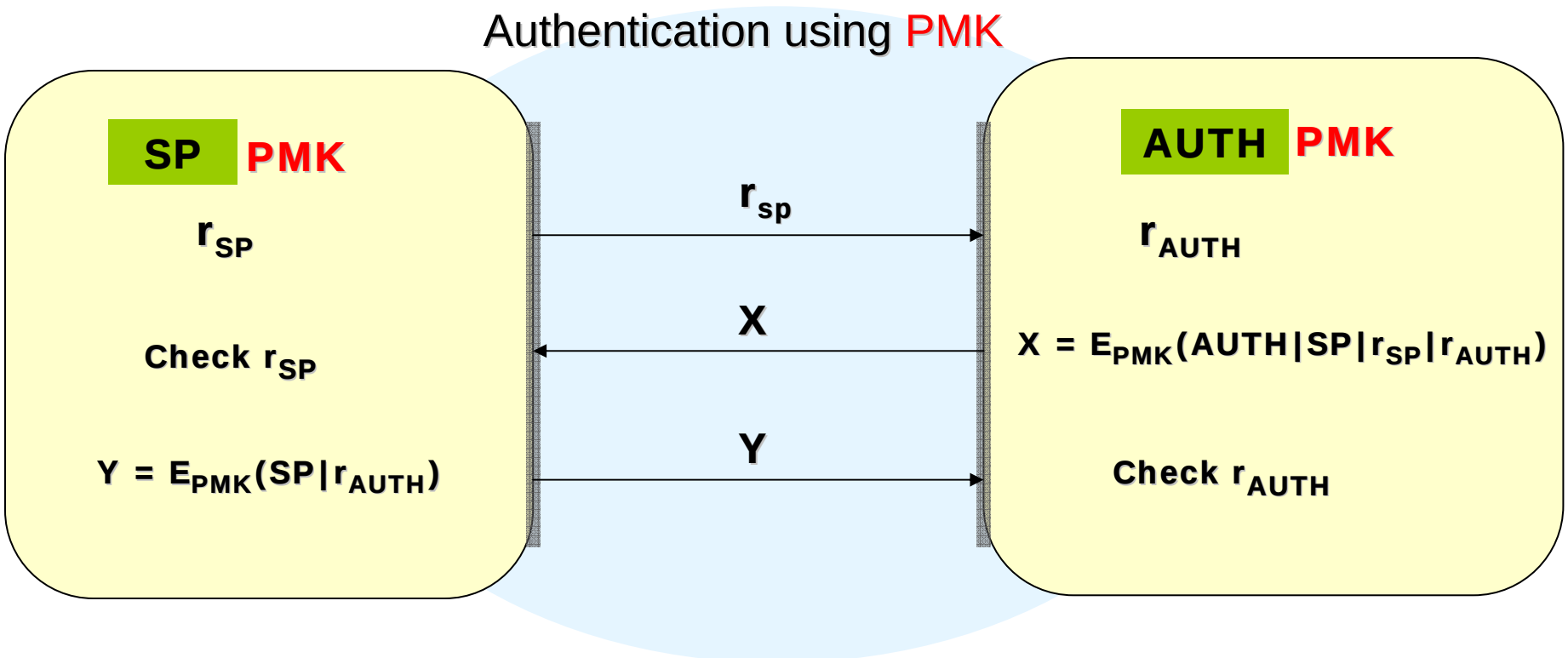
- SP : Supplicant
- AUTH : Authenticator



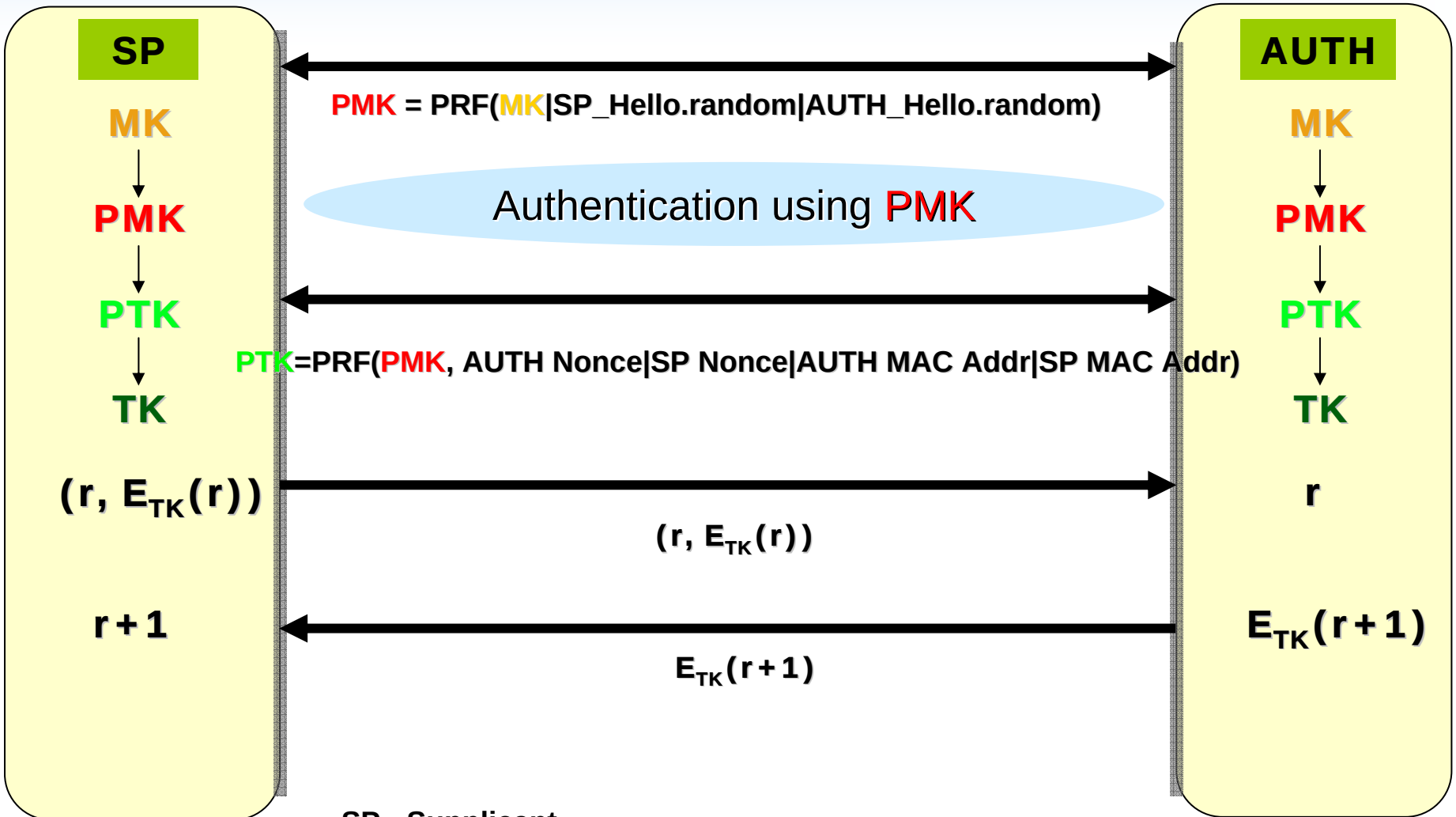
Authentication

•SP : Supplicant
•AUTH : Authenticator

- 802.1x is so bulky for Layer 2 Authentication
- Using Pairwise Mater Key (PMK)
  - Make it Simple



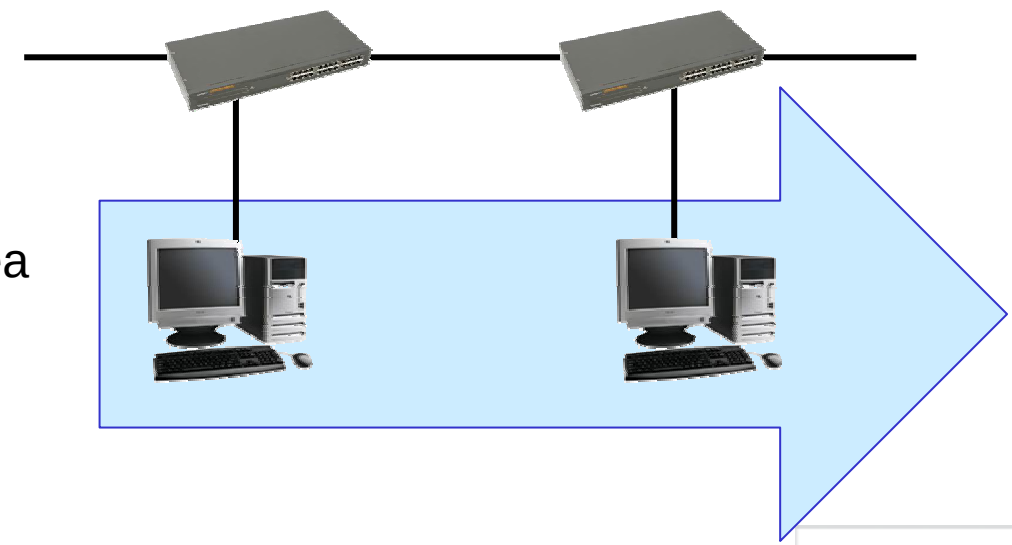
Key Exchange with verification



- SP : Supplicant
- AUTH : Authenticator

Mobility

- **Glossary**
  - In the networks, the ability of a terminal, while in motion, to access telecommunication services from different locations, and the capability of the network to identify and locate that terminal.
- **Considerations**
  - Wireless Supplicant always needs mobility
  - Wired Supplicant
    - Frequency
    - Scope
      - Bridge to Bridge
      - Over the local area

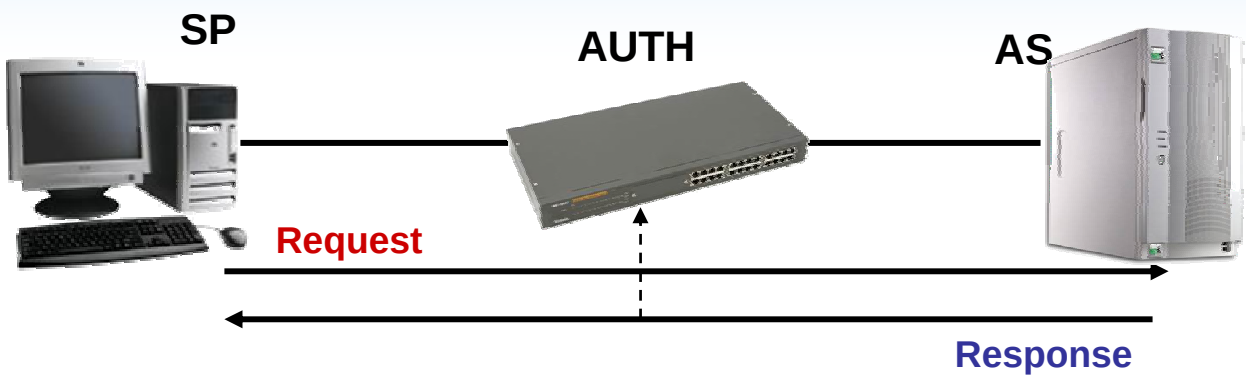


Ensuring Mobility (1/2)

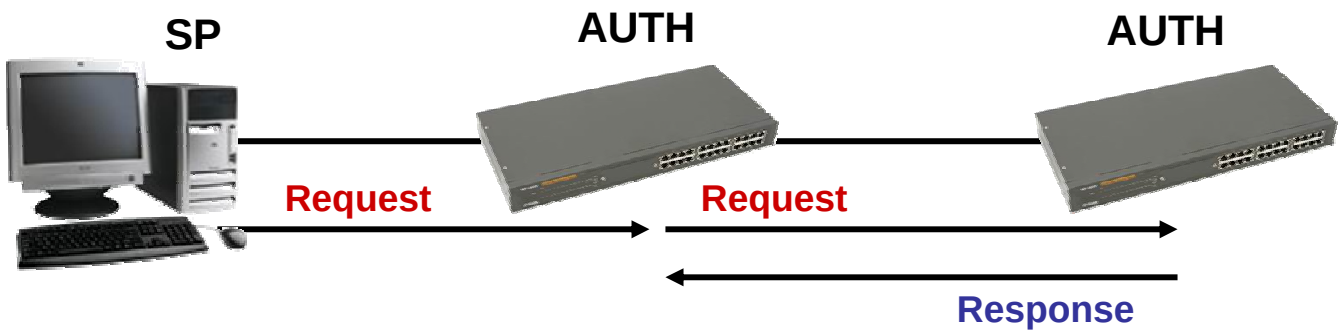
- **Requirements**
  - Require a system whose role works like Authentication Server (AS)
  - Guarantee communication channel with Layer 2 protocol
- **Possible Models**
  - Back-end [1]
    - Relay role between Supplicant (SP) and AS
    - Watch the response from AS to SP → set controlled port
    - Whether SP includes Authenticator Address information or not
    - The key distribution protocol for making AS know SP's
  - Authenticator (AUTH) + AS [2]
    - Subject of authentication : AUTH
    - Protocol for finding the authentication information of SP
      - Broadcast
      - Query with Destination MAC Address
  - Assumptions
    - globally unique MAC address
    - AS (or AUTH) maintains master key information table between SP address and AUTH address
    - Pre-established secure channel among AS (or AUTH)

Ensuring Mobility (2/2)

[1]



[2]



- Further works
  - ➔ Key Management to support mobility

Thank you for your attention

Q&A