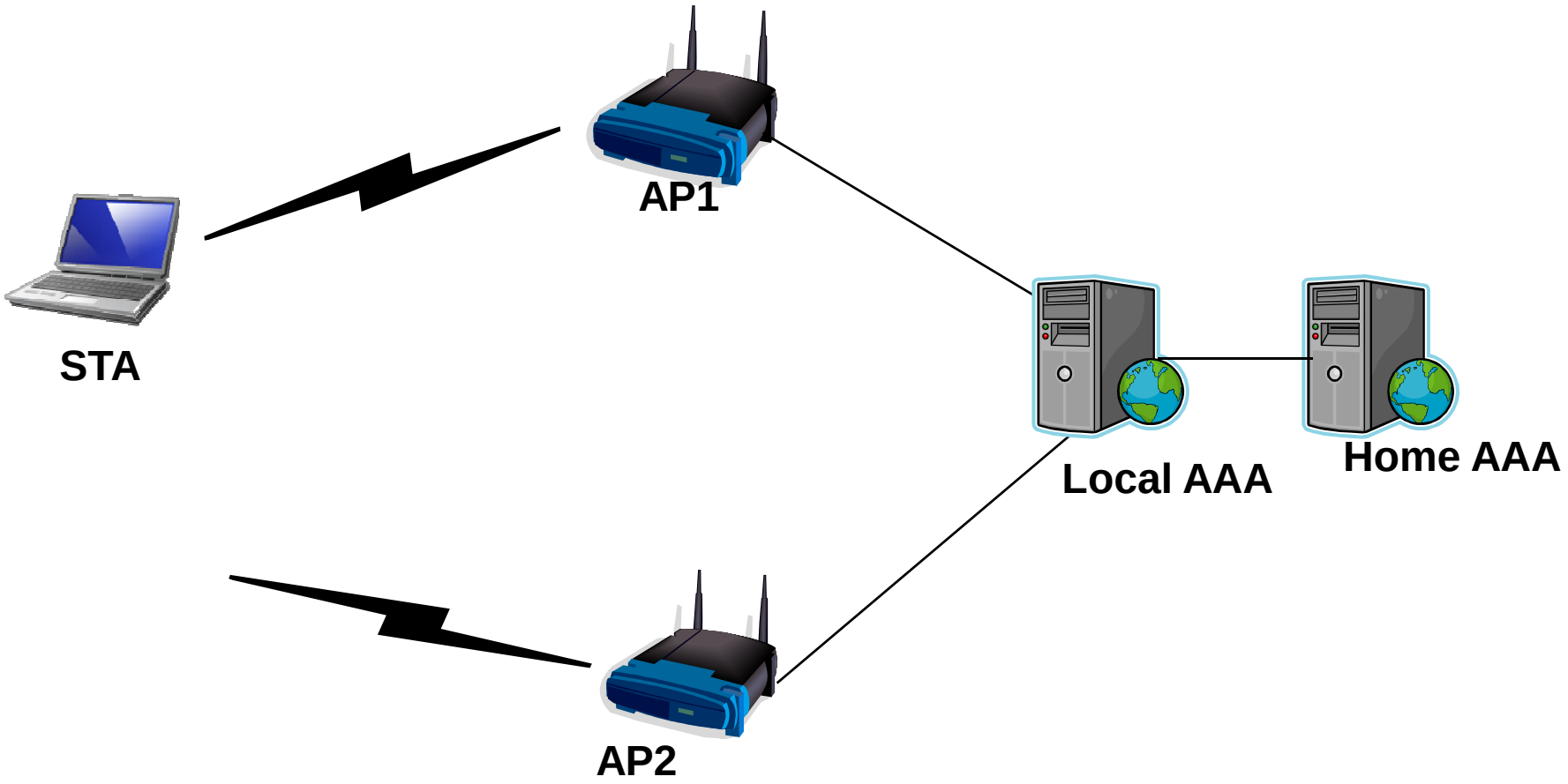
ERP IMPLEMENTATION

Kedar Gaonkar

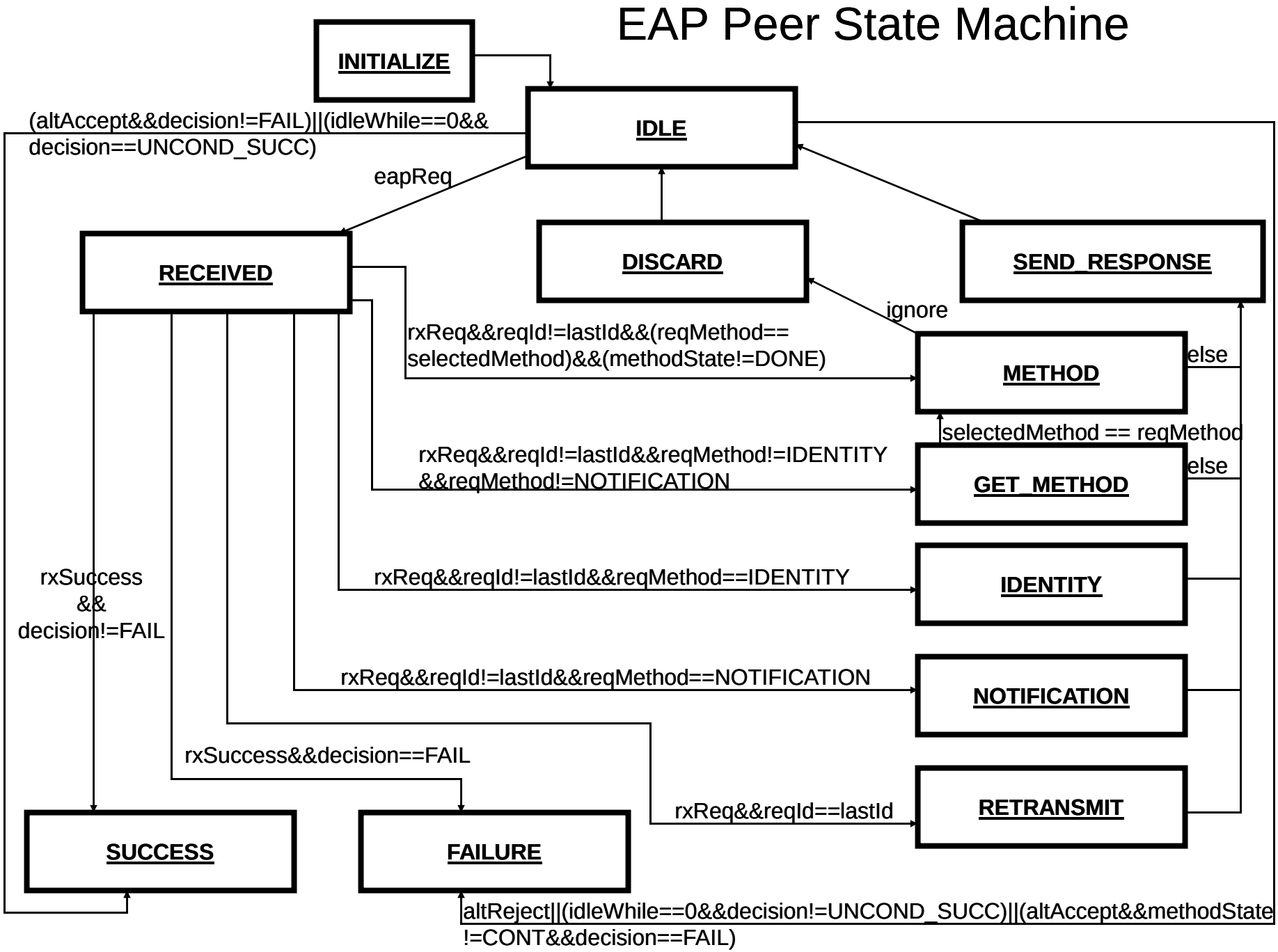
IETF-69 Chicago, July 23rd, 2007

Deployment Scenario

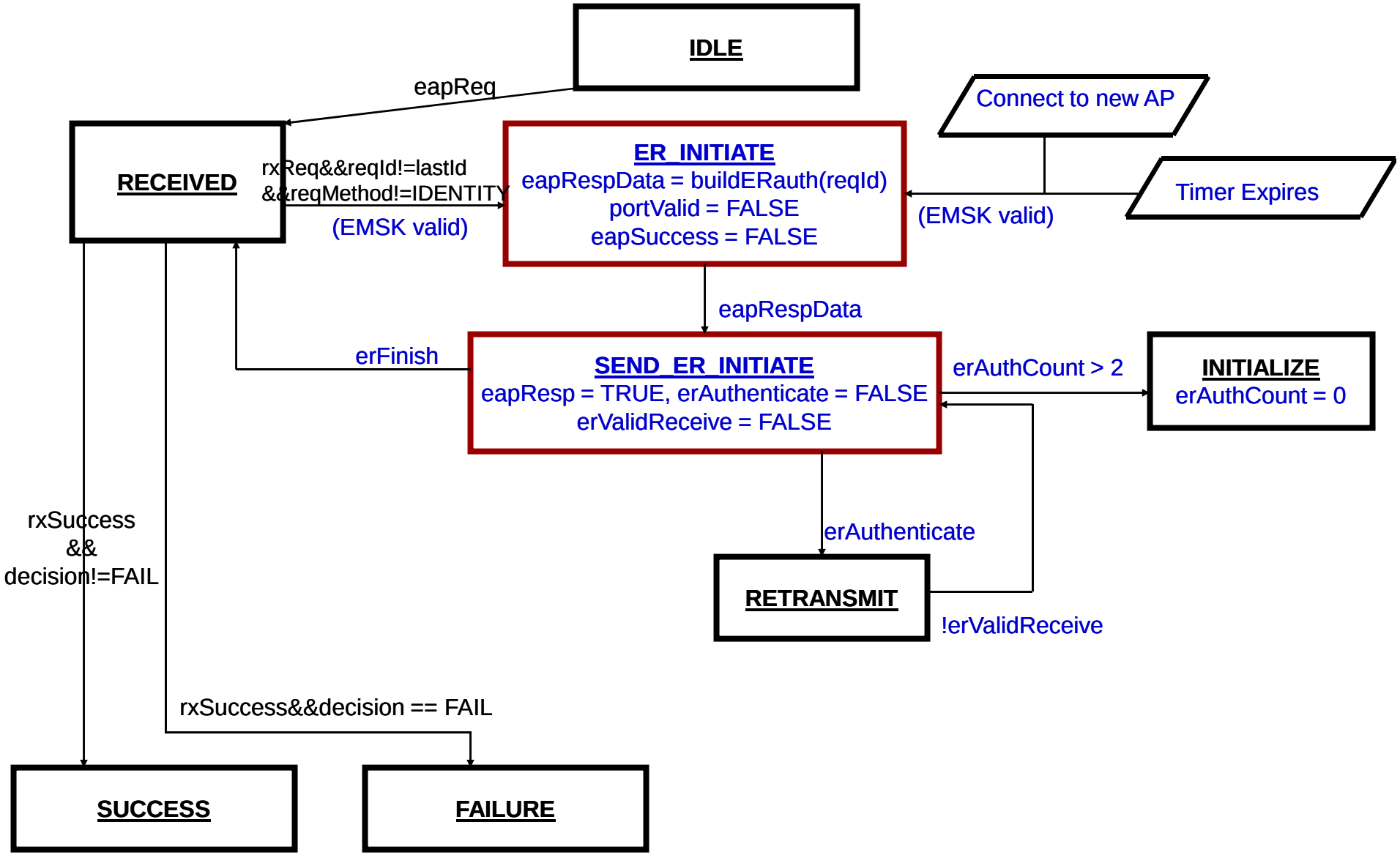


Implementation

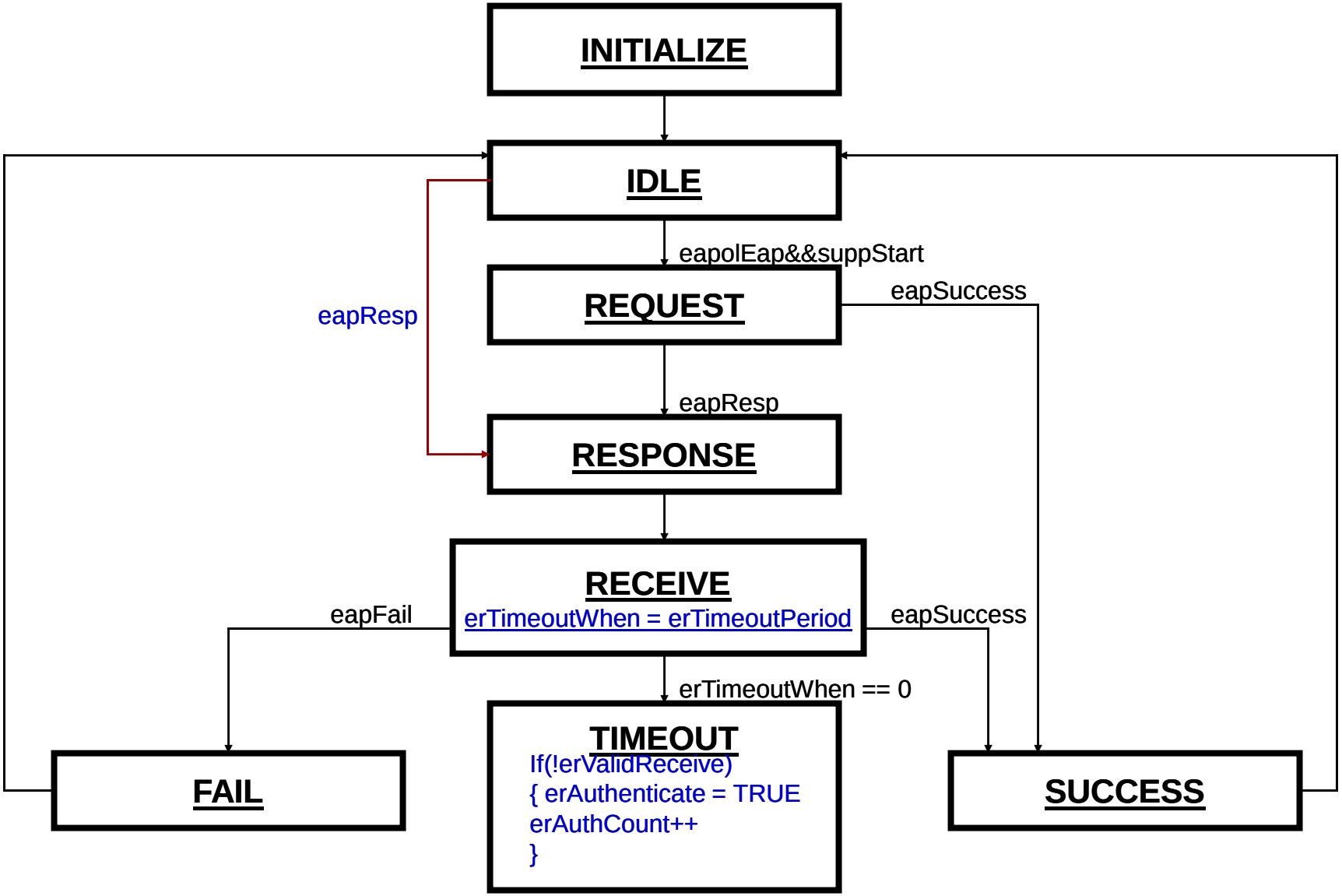
- **Setup consists of 4 machines: Supplicant (STA), Access Point (AP), and Local AAA Server, and Home AAA Server**
  - **‘wpa_supplicant – 0.5.7’ at Supplicant**
  - **‘HostAP – 0.5.7’ at Access Point**
  - **RADIUS implemented at AS by using ‘freeRADIUS – 1.1.6’**
- **EAP-TLS selected as the EAP method**
- **OpenSSL used to generate certificates**
- **STA associates with AP wirelessly through DWL-G650 network cards (Atheros Chipset)**
- **AP is connected to Local AAA by a CAT5 cross-cable**
- **Local AAA and Home AAA exist on common LAN.**


EAP Peer State Machine
INITIALIZE
IDLE
(altAccept&&decision!=FAIL)||(idleWhile==0&&
decision==UNCOND_SUCC)
eapReq
RECEIVED
DISCARD
SEND_RESPONSE
ignore
rxReq&&reqId!=lastId&&(reqMethod==
selectedMethod)&&(methodState!=DONE)
METHOD
else
selectedMethod == reqMethod
rxReq&&reqId!=lastId&&reqMethod!=IDENTITY
&&reqMethod!=NOTIFICATION
GET_METHOD
else
rxSuccess
&&
decision!=FAIL
rxReq&&reqId!=lastId&&reqMethod==IDENTITY
IDENTITY
rxReq&&reqId!=lastId&&reqMethod==NOTIFICATION
NOTIFICATION
rxSuccess&&decision==FAIL
rxReq&&reqId==lastId
RETRANSMIT
SUCCESS
FAILURE
altReject||(idleWhile==0&&decision!=UNCOND_SUCC)||(altAccept&&methodState
!=CONT&&decision==FAIL)

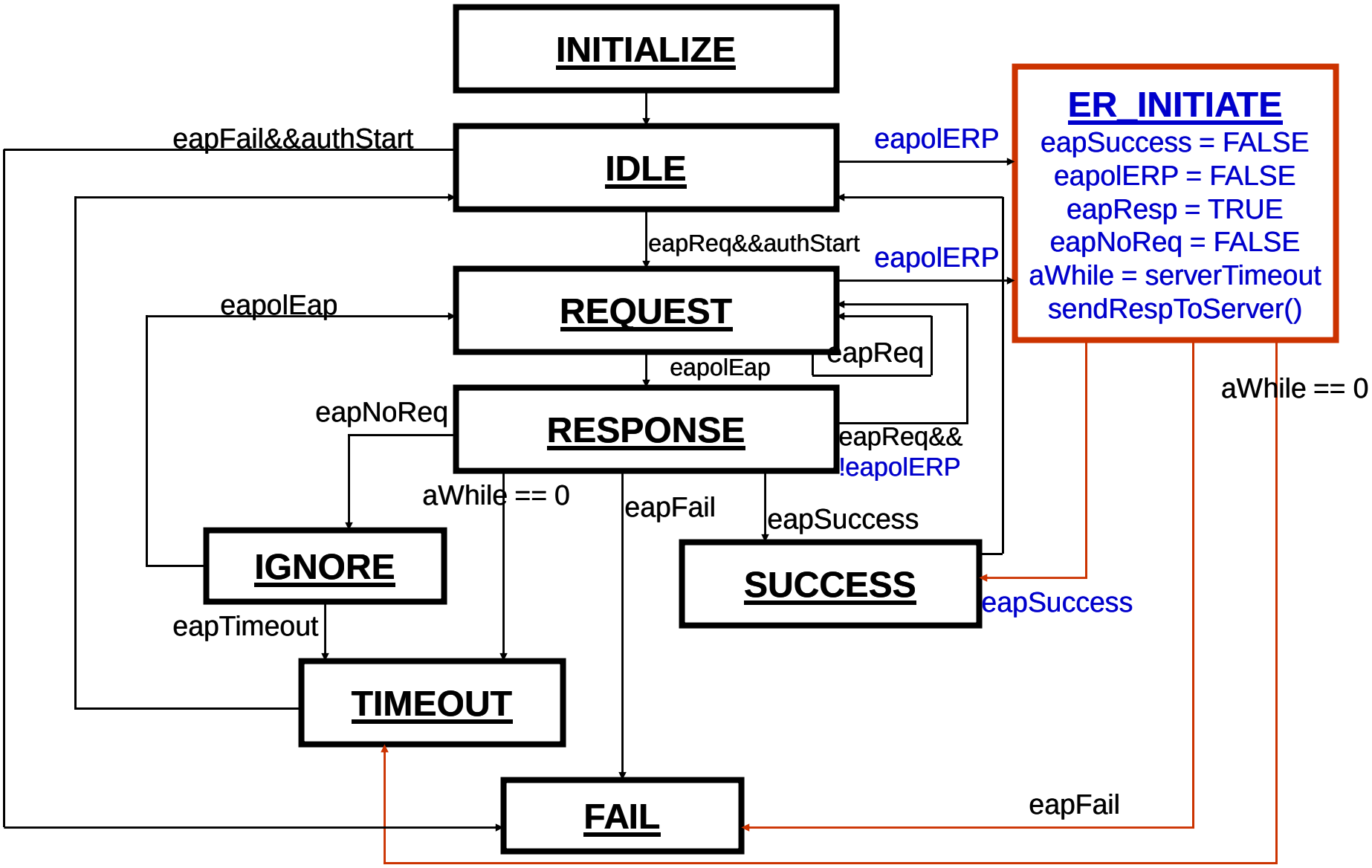
Peer ERP State Machine



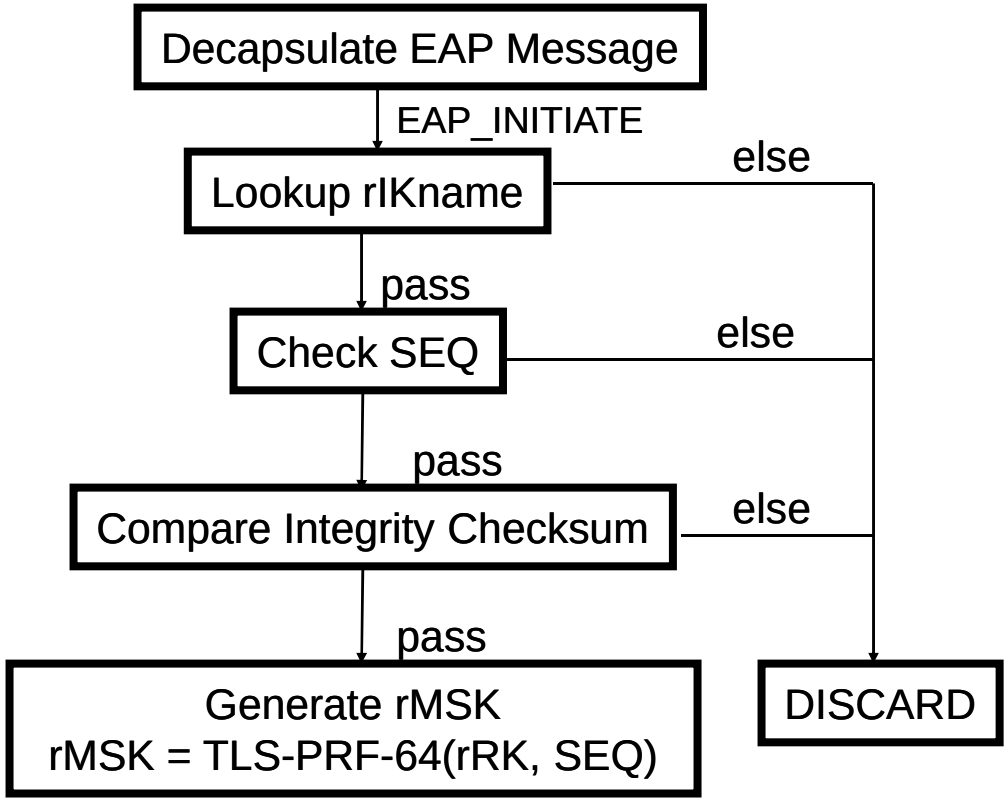
Peer Eapol Backend State Machine



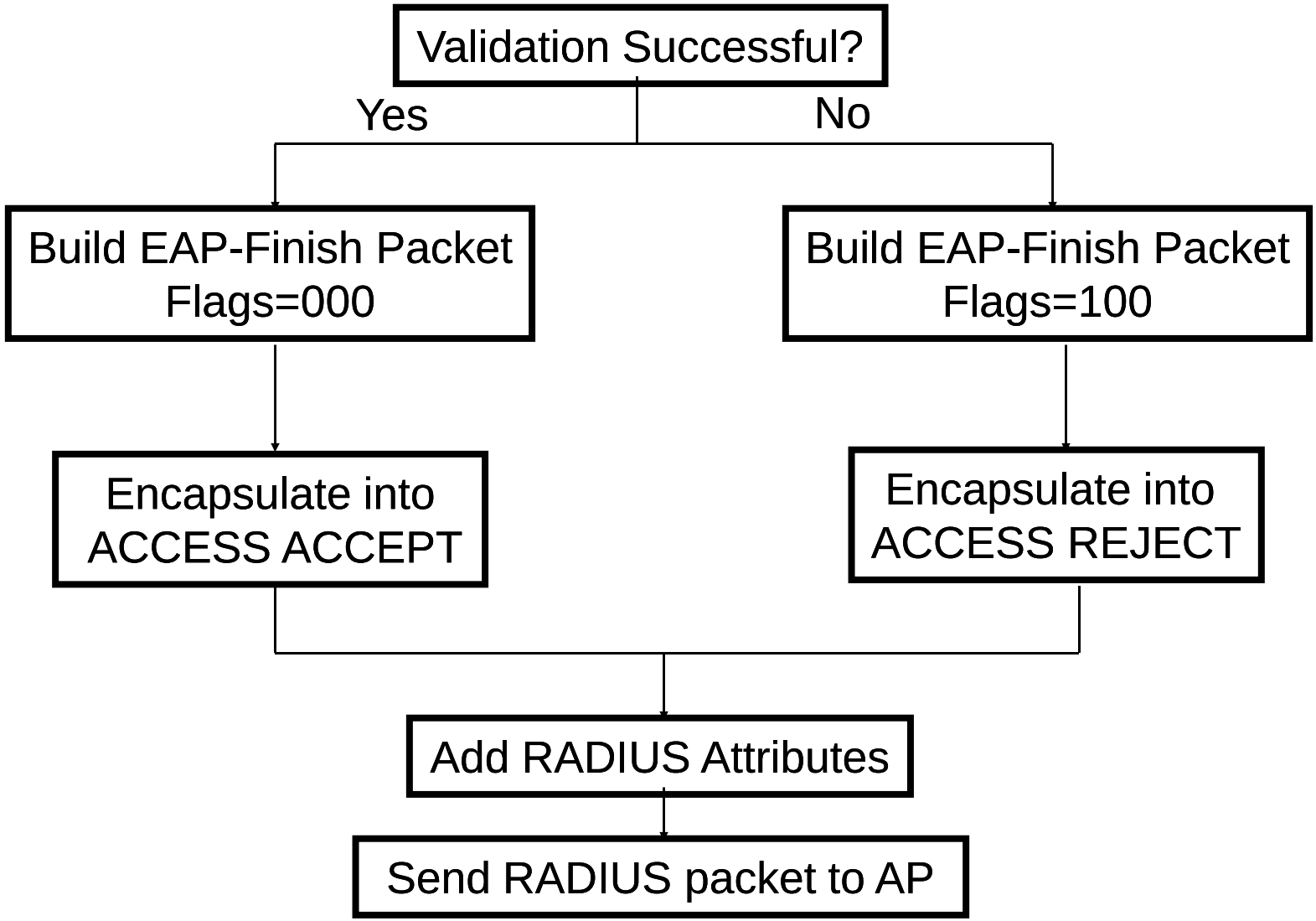
Authenticator EAPOL State Machine



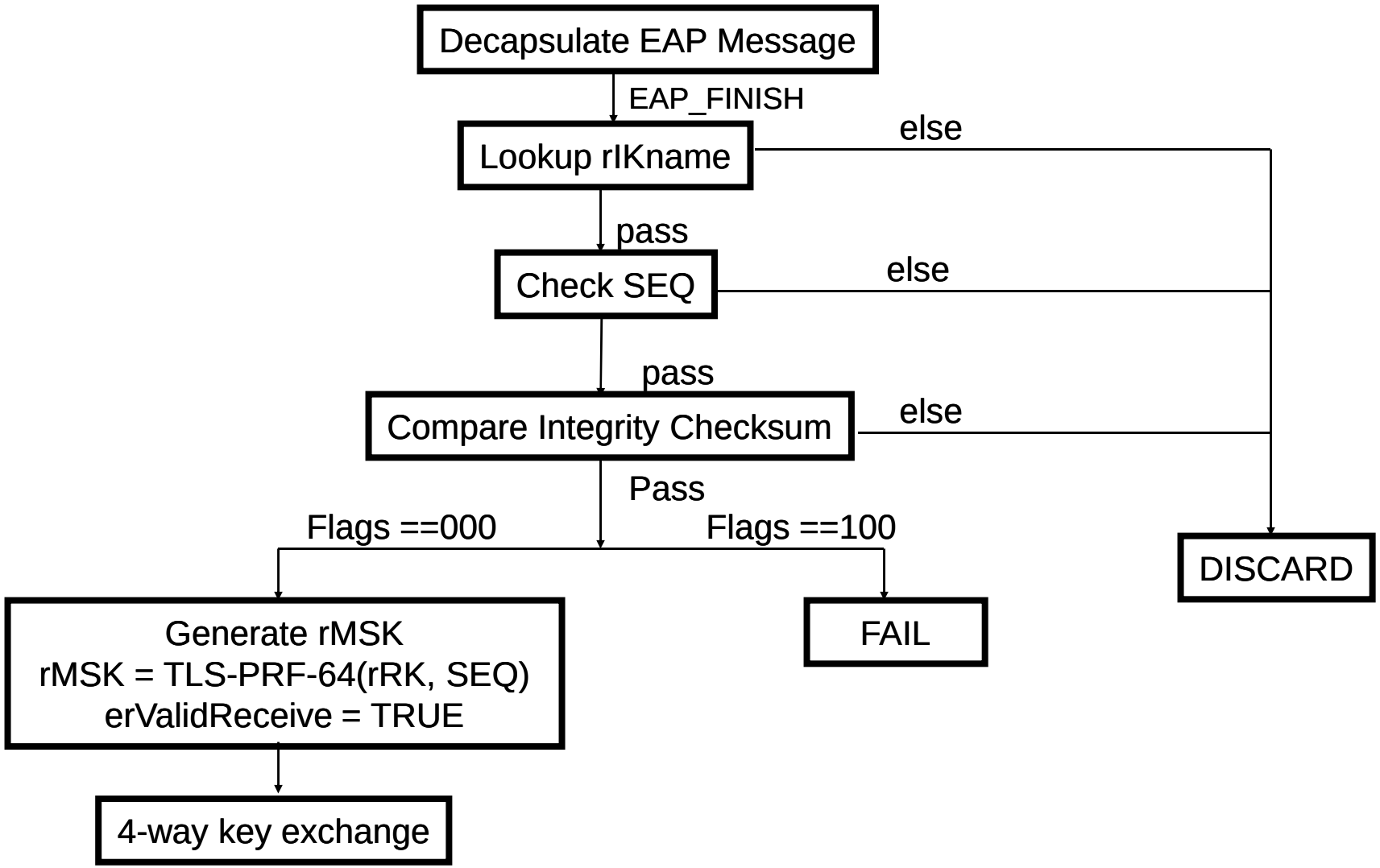
Message Validation and Key Derivation at AS



Send EAP_FINISH to AP



Message Validation and Key Derivation at Peer

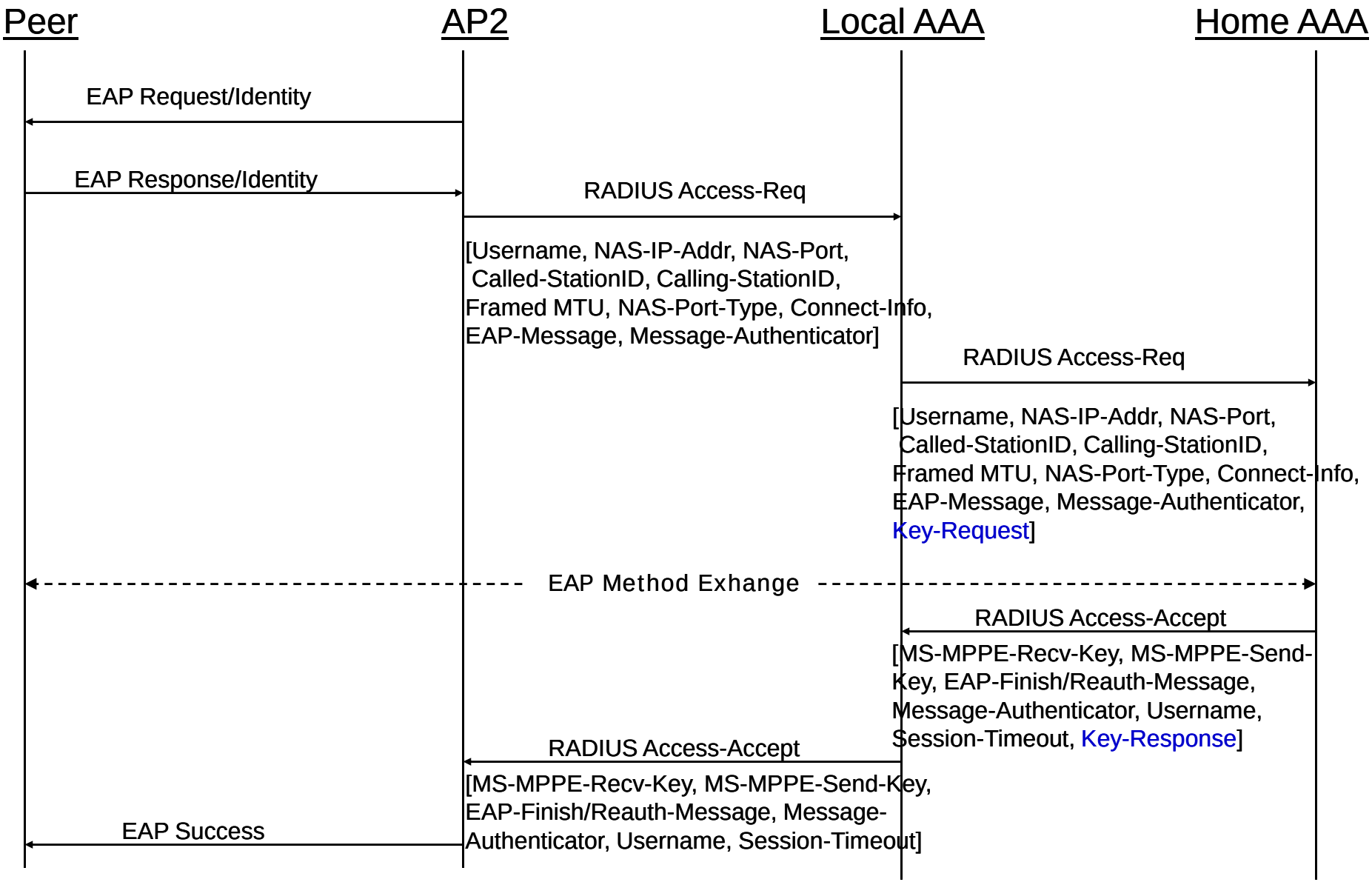


New RADIUS attributes proposed

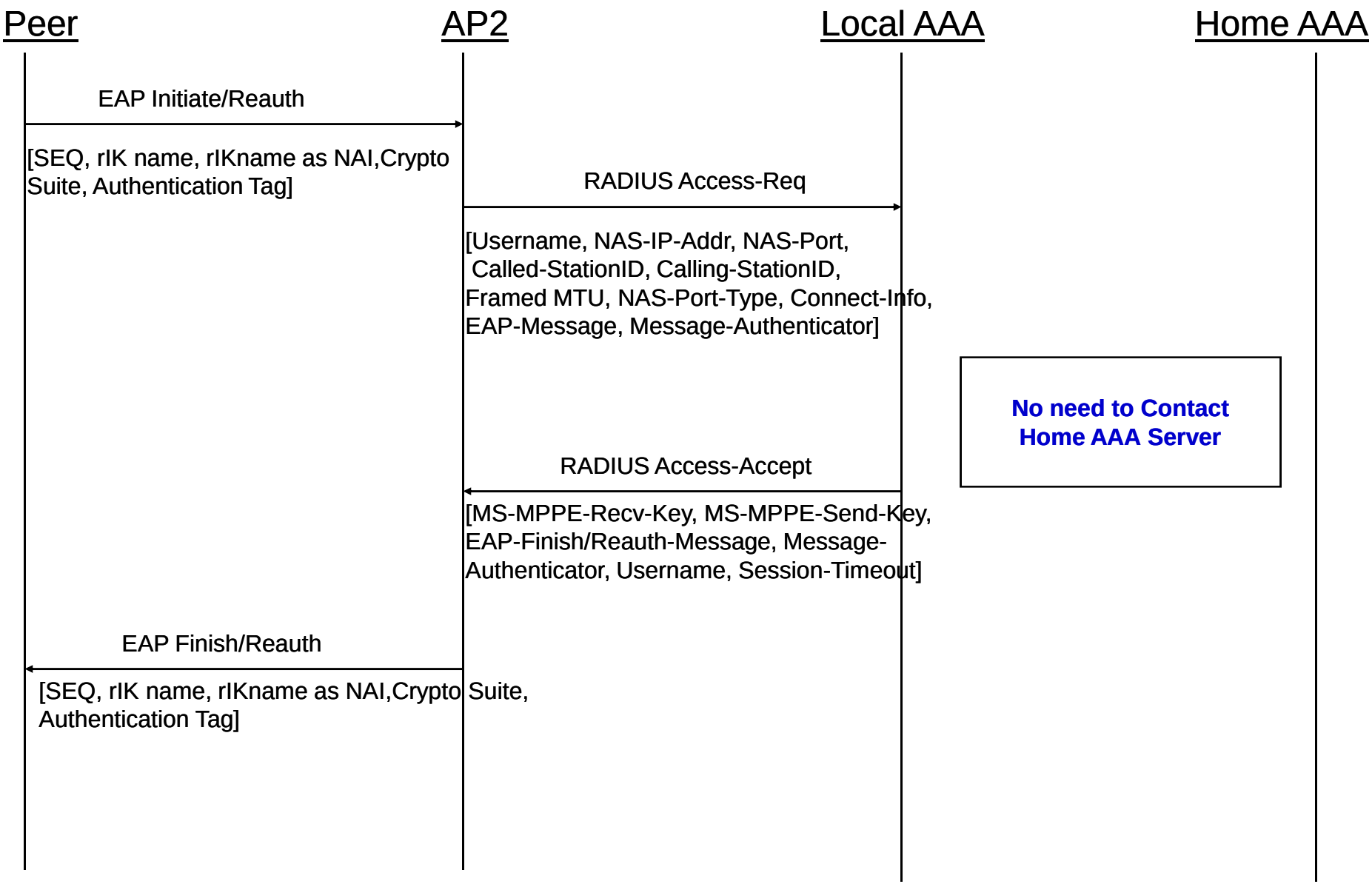
- **Local AAA server requests key from Home AAA server**

- **Two new RADIUS Attributes:**
  - **Key-Request Attribute**
  - **Key-Response Attribute**

Initial EAP exchange



During ERP Reauthentication



Acknowledgments

- freeRADIUS Team

- Host AP and wpa_supplicant : Jouni Malinen

Thank You!

Questions?