Authentication and Privacy in EPON

Jin Kim

Samsung

IEEE802.3ah, Vancouver, July ,2002

What security services needed for EPON?

- ‘Broadcast and select’ topology for downlink
  => Privacy (encryption for downstream packet)

- Unauthorized or masquerading ONU in EPON
  => Authentication
  and encryption with authenticated key for upstream packet
  “ I am not only physically connected, but also the right one”
  -> registration -> authentication

security algorithms and other common security issues are to be discussed in other standard body for security

Issues

- **Authentication**
  - Various granularity level of security service
    ; authentication to ONU, logical link port, user ?
  - Authentication Protocol: 802.1x ? (see Appendix)
  - Authentication/key management layer: 802.1x?

- **Key management**
  - different key to each logical link?; MPCP per LLID
  - different key to each ONU? ; use multicast ID as ONU-ID
    or single LLID per ONU
  - key synchronization method (see Appendix)
  - encryption key derivation / session key generation
  - key distribution MPCP and message format
  - key distribution for multicast group
    ; releasing members from a multicast group is done by rekeying all other members

- **Privacy**
  - encryption algorithm ; AES – OCB mode? (see Appendix)
  - encryption layer and content fields to be encrypted

Is it so…..?

1. **Is any info. in preamble robust against eavesdropping?**

   ; marginal advantage in security, big disadvantage in compatibility

   - HW and decoding tools will emerge for good and bad reasons

   - new HW means that EPON-dedicated-HW cannot serve for other Ethernet topology (no compatibility), which is a risk factor unfavorable to service providers and chip manufacturers, instead.

2. **Can encrypting DA/SA do the protection of MAC address?**

   ; DA/SA is exposed anyway :

   - in the region from the subscriber ports in ONU to users (802.11, 802.16 and other LANs don't encrypt DA/SA)
   - in Auto Discovery Stage
   - when packet is transmitted with 'encryption-off' flag (ex. MPCP message distributing public keys MPCP message using authentication mechanism PAP w/802.1x

   ; better resort to random conversion of MAC add. or other methods to support anonymity

Is it so…..?

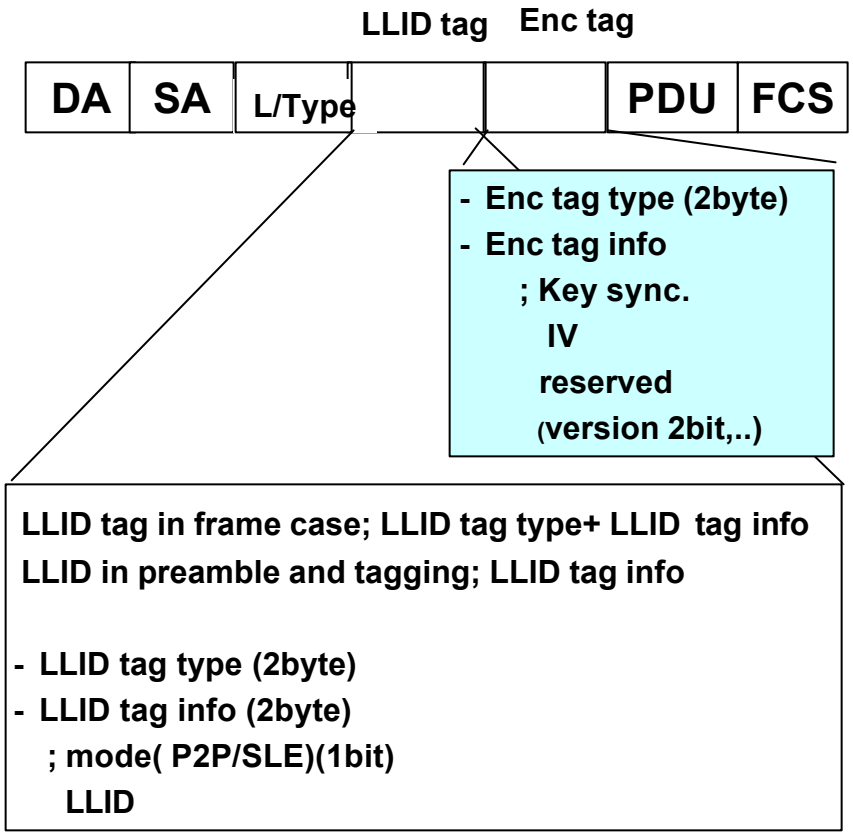
3. Is Encryption layer above RS layer has advantages over encryption above MAC layer?

- MPCP for key management is performed by MAC client (or 802.1x layer)
- Decision on enc-on/off for encryption flag is triggered by MAC client

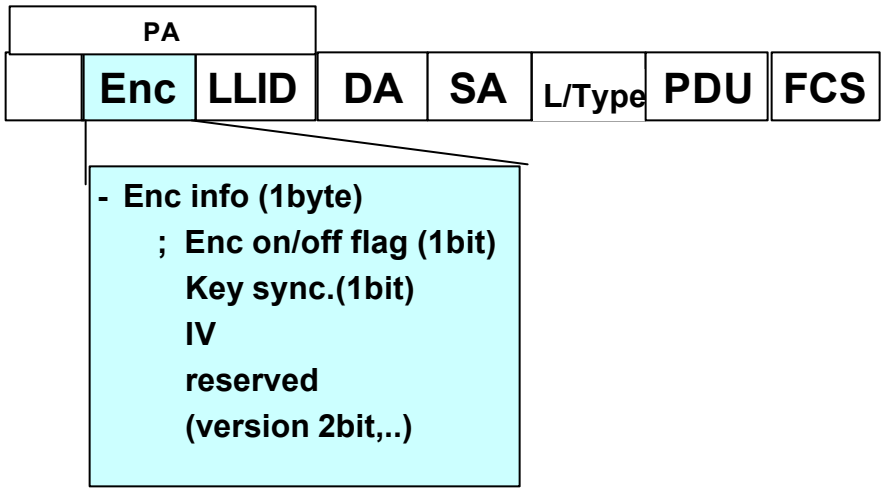
; In case of Enc. layer above RS, those info. need to be passed down from MAC client to Enc. layer above RS,and info. in preamble need to be delivered to the key management block. Lots of primitives need to be defined for this operation

Message format

<Enc tag in frame>



<Enc tag in preamble>



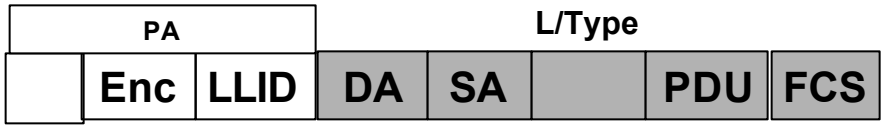
Is length of preamble enough to convey
; SOP(1byte)+ CRC(1byte)+Enc(1byte)
+LLID(2byte)+OAM(1byte)+ further fns?

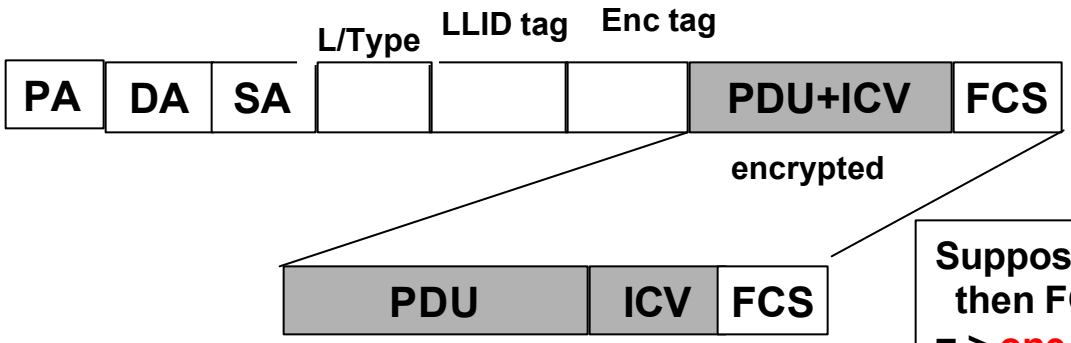
- some modes of encryption operation require IV(initialization vector)
- in Enc tag in frame case, the packet with an Enc tag means that the packet is encrypted, and the packet w/o an Enc tag means it is not encrypted
- Clause 4; maxTaggedFrameSize = (maxUntaggedFrameSize + qTagPrefixSize)

Data integrity

< Enc at MAC client >
(Encrypting PDU)

< Enc above RS layer >
(Encrypting DA~FCS)





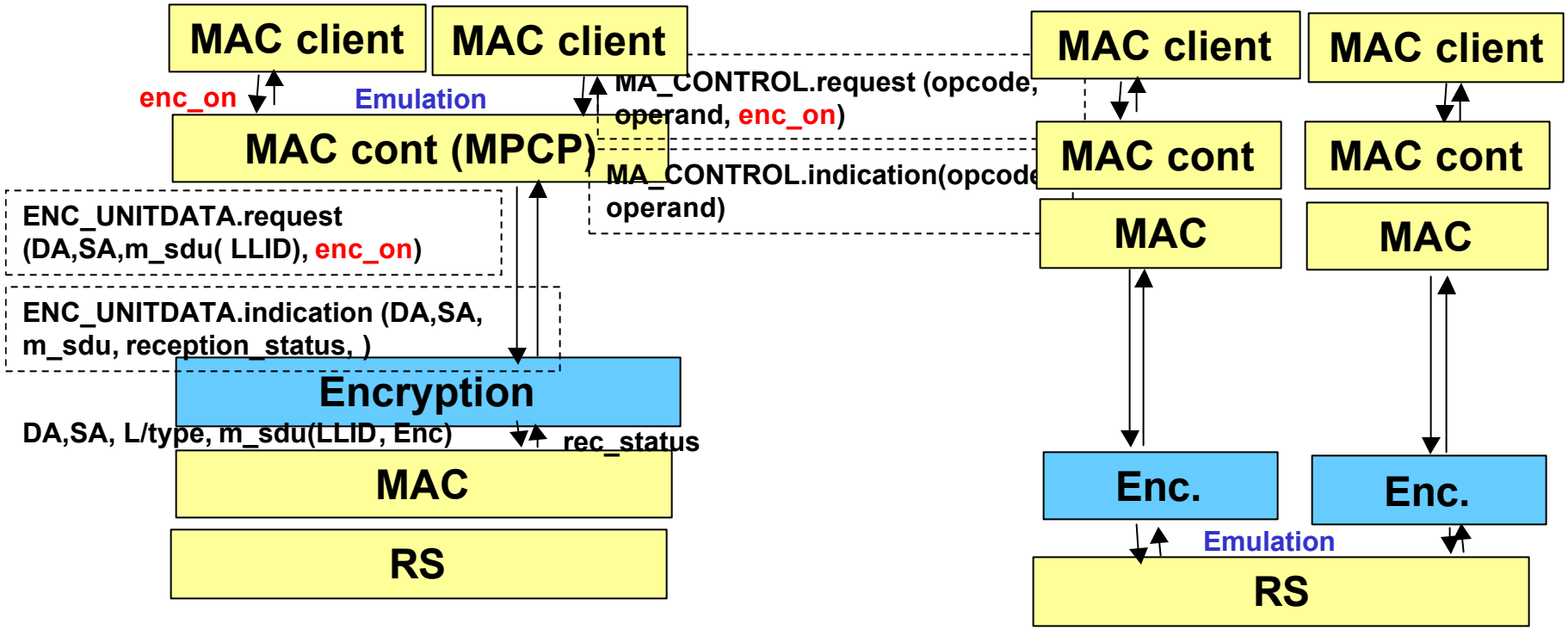
Suppose link error in encrypted message (DA~FCS), then FCS check error occurs
= > one can't tell whether it results from link error or from wrong key encryption
=> Link management problem and can't decide on message authentication

ICV (integrity Check Value) ; check sum(4byte) if using AES-OCB(802.11i)
If FCS (of ciphered PDU+ICV)≠ FCS ; link error
after decrypted at Encryption layer
If ICV (of deciphered PDU) ≠ ICV; wrong key encryption

Encryption on/off

< Enc at MAC client >

< Enc above RS layer >

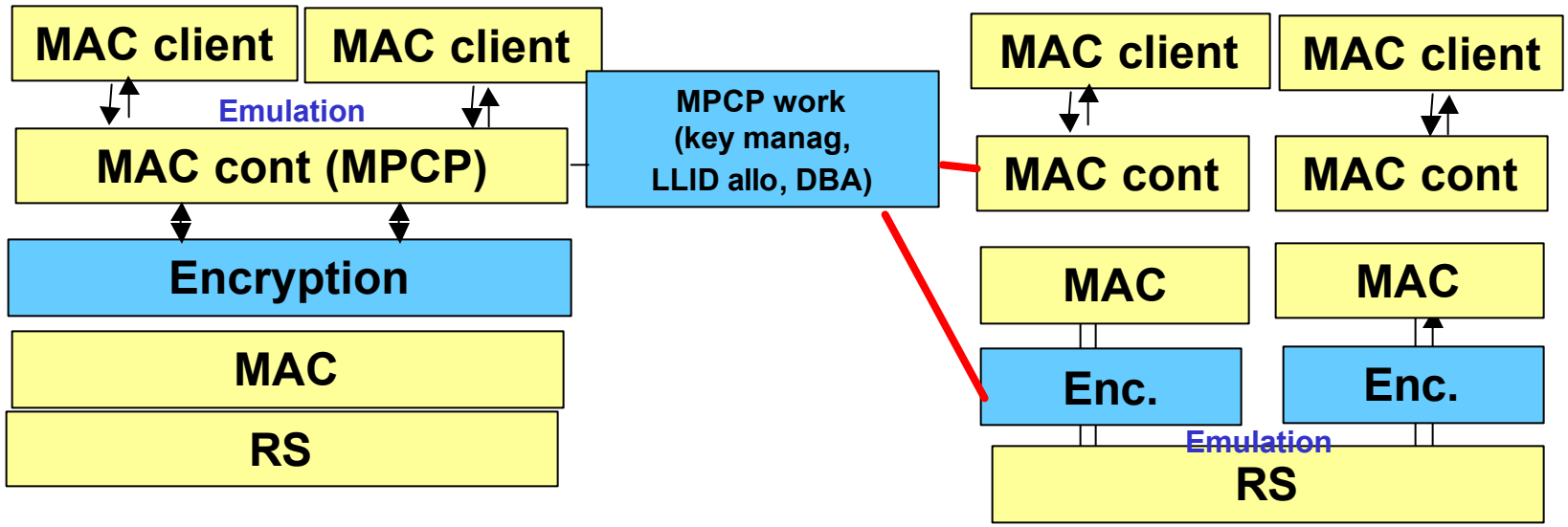


- Enc_on is triggered by MAC client
- How is this info passed to the Enc. Layer ?

Encryption layering

< Enc at MAC client >

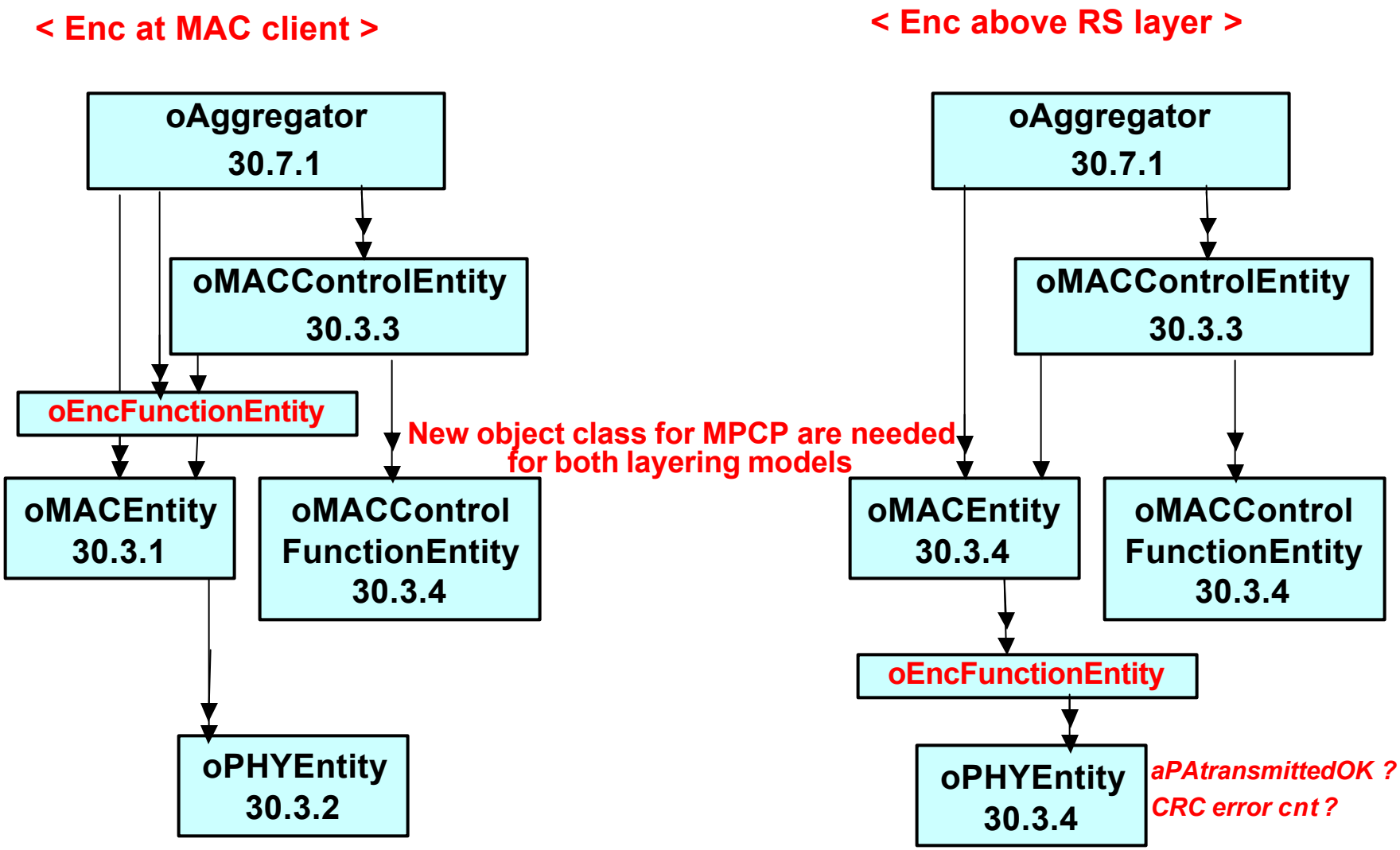
< Enc above RS layer >



- MPCP for key management is performed at MAC control layer
- then how can Enc info (like key for LLID) from MAC client be delivered to Enc. layer w/o passing thru MAC?
- - For this, 802.3 must be modified in Enc above RS layer model

(info. passed between state machines must be defined by primitives. ex. How to implement interfaces to operand-list-registry for Pause operation is vendor-specific . Nevertheless, primitives (operand) from MAC control to MAC client had to be defined in 802.3)

Link management



Conclusion

- “ security is a risk management problem”

  ; Optimize between risk reduction and complexity/cost increase since risk exposure to a certain extend is accepted

  - New PHY HW for Enc and LLID in preamble and complex MPCP for obscuring LLID and MAC address also have the price to pay
  - no encryption of DA/SA seems acceptable as in other networks

- Enc. and LLID in frame and Enc. layer above MAC is the effective solution for passing the Enc info (such as encryption_on/off from MAC client, key from MPCP engine for LLID allocation and key management at MAC client) to the Enc. layer.

  (Enc. above RS layer requires lots of primitive modification for this operation)

Further work

- Choose encryption algorithm to hook

  - message format, key management mechanism may be dependent of the encryption engine

  - analyze selected/alternative algorithms in terms of processing/BW overhead, robustness vs. vol.

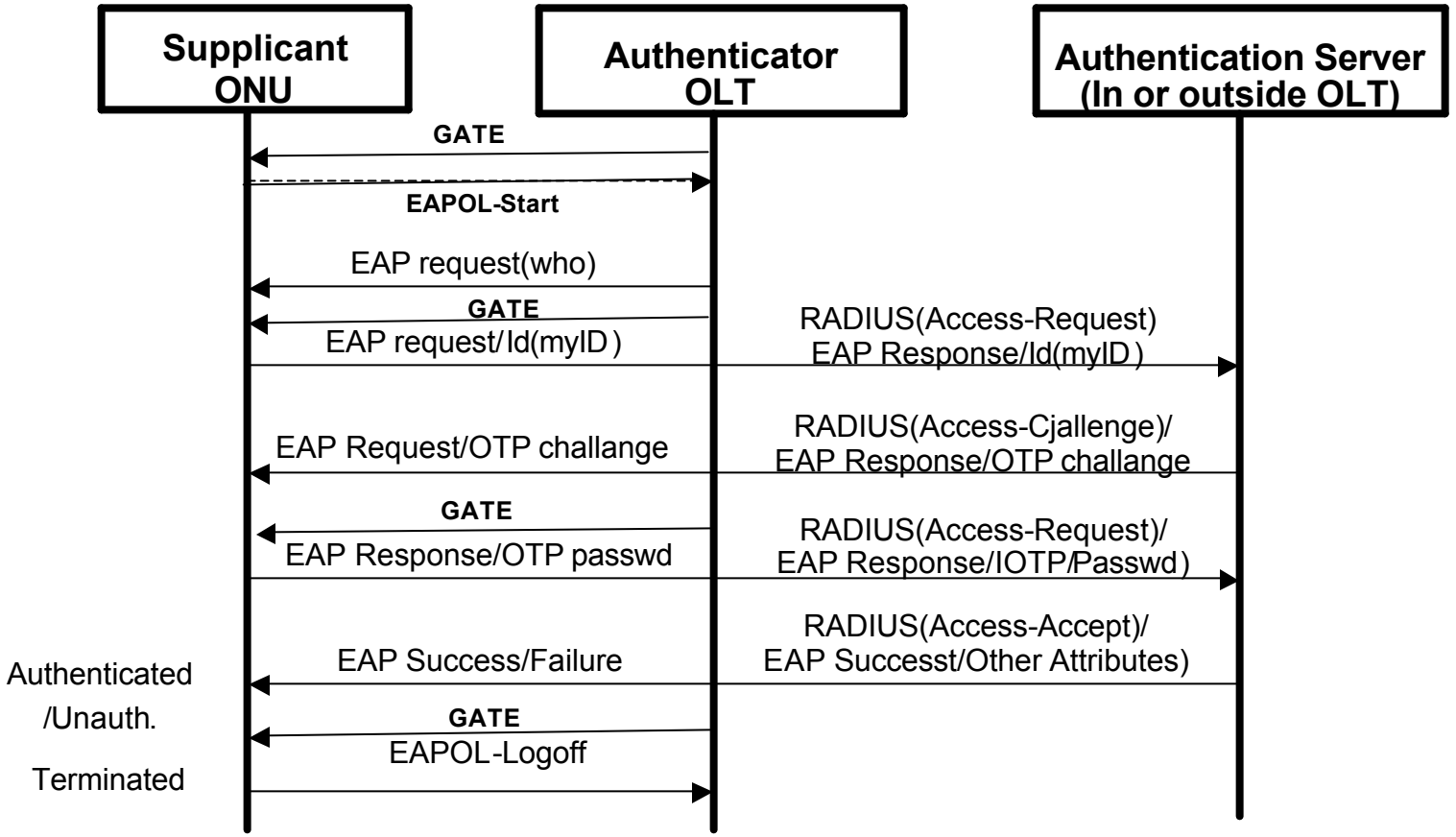
- Define frame format and MPCP for key management ; opcodes for New_key_request/response, and etc.
- Define primitives and state machines for security functions

Authentication

Appendix

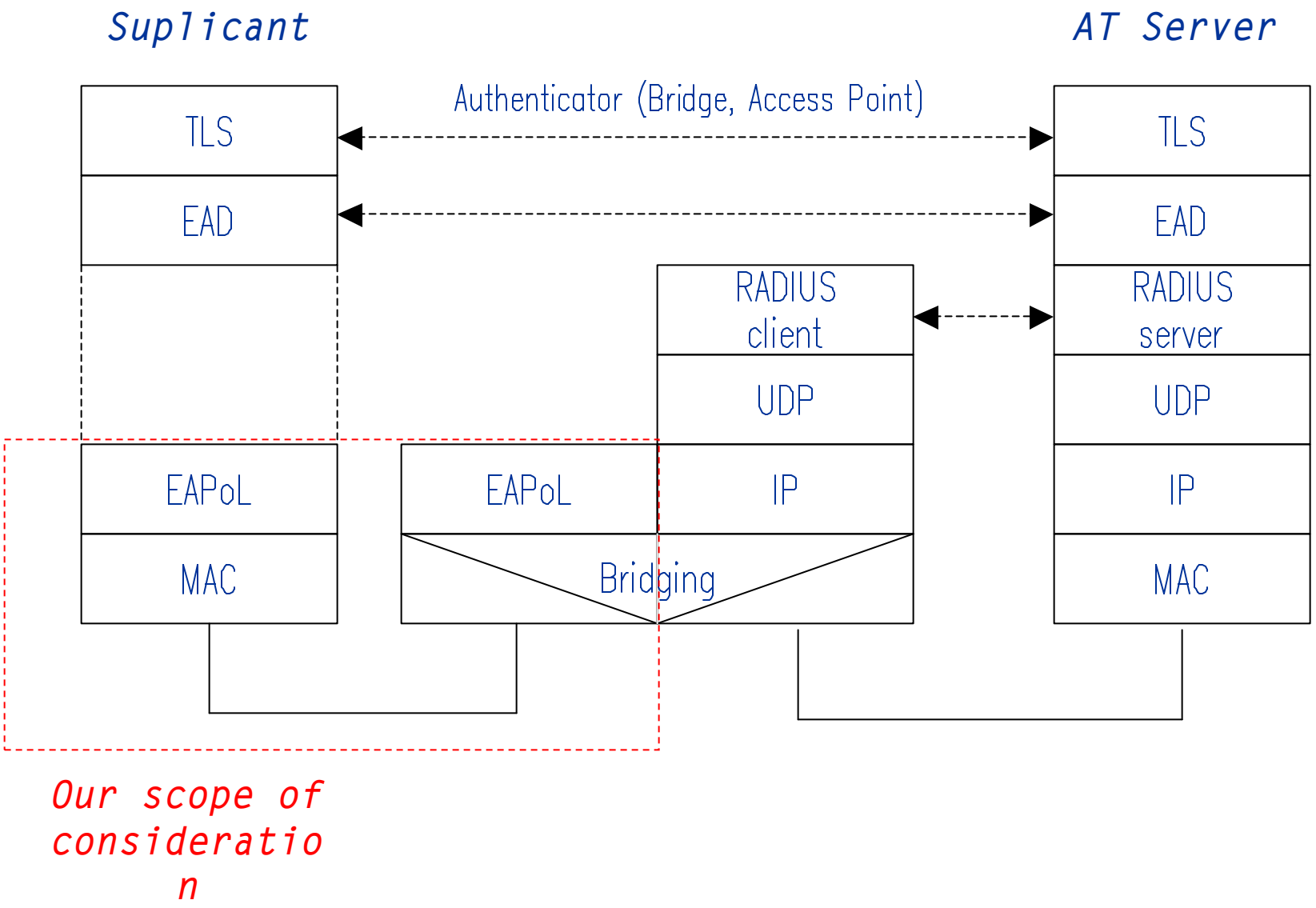
An Option based on Kerberos over 802.1x ; Extensible Authentication Protocol(EAP)

- **EAP encapsulation with L/Type of 88-8E**
- **Authentication is performed after/during registration**
- **ONU may initiate the process (ONU pre-registered in AS and having ID, passwd)**



Layering of Authentication of 802.1x

Appendix



Key Management
; Key Distribution and Synchronization *Appendix*

Periodic rekeying by distributing a random number encrypted with a secret key

Rekeying period : churning (APON); every 2 sec

DES (DOSIS) ; every 12 hours

WEP(802.11) ; every transmitted packet

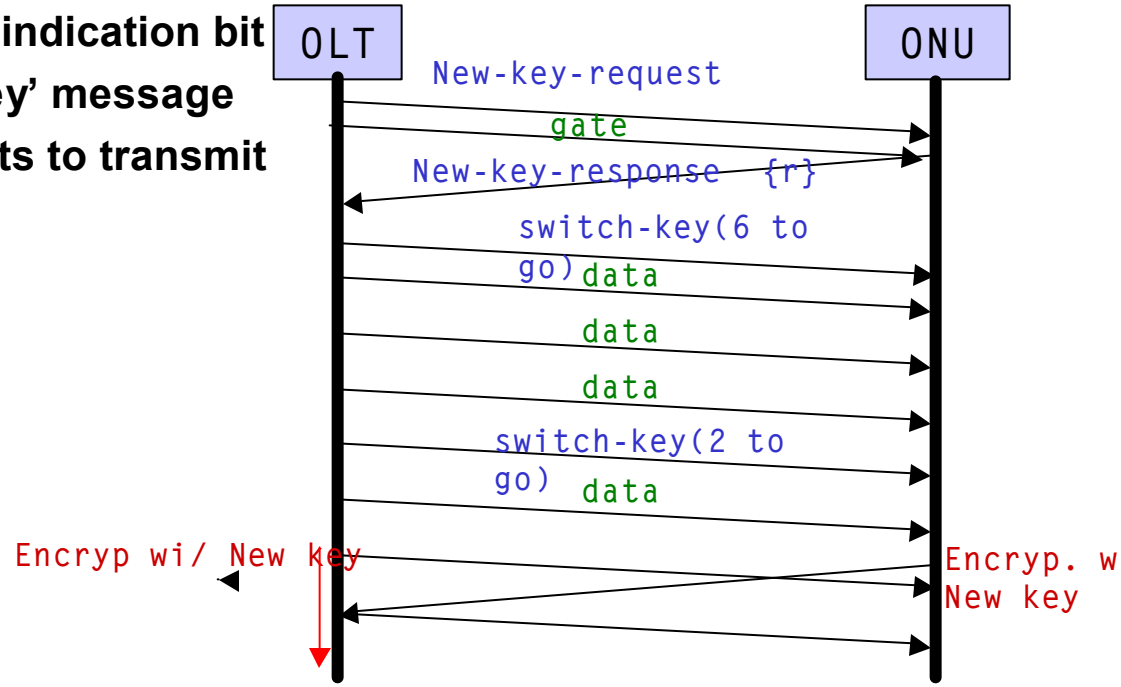
AES 128bit (802.11i) ; $3*10^{17}$ years

Key synchronization methods

; option 1. key distribution acknowledged

2. toggling by switch_key indication bit

3. OLT sends a ‘ switch-key’ message with the number of packets to transmit until switching

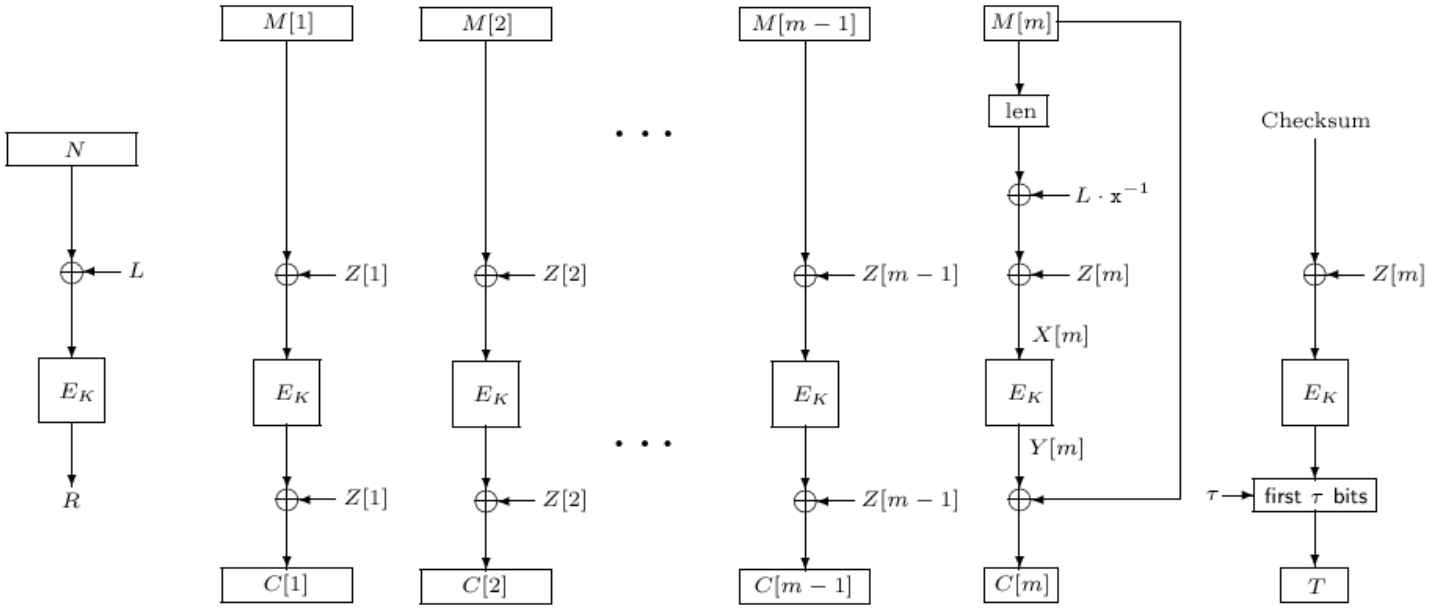


Encryption Algorithm

Appendix

An Option based on 802.11i ; AES-OCB mode

- **AES (Rijndael) ; symmetric block cipher**
  data block, key length: 128,192 or 256bit
  no last block problem
- **OCB mode ; parallel processing**
  support privacy and integrity (integrity algorithm included)



Integrity

***T* (=32 or 82) bit extension**