Encryption layer comparison

Yannick Le Goff, France Telecom
Yukihiro Fujimoto, NTT
Ken Murakami, Mitsubishi Electric
Onn Haran, Passave
Olli-Pekka Hiironen, Nokia

Encryption options

- RS
  - Encryption functions on Emulation sub-layer
  - 3 indications is preamble
  - Full frame (DA - FCS) encrypted
- MAC control with MIC field
  - Encryption functions on lower part of MAC control
  - ENC tag [2 bytes] inserted to frame, includes 2 indications
  - Payload encrypted
  - Message Integrity Code (MIC) [4 bytes] inserted before FCS field
- MAC control without MIC field
  - Encryption functions on lower part of MAC control
  - ENC tag [2 bytes] inserted to frame, includes 2 indications
  - Payload encrypted
- IPsec
  - IPsec tunnel between OLT and ONU
  - Encryption and message authentication

Security objectives

- Authentication
  - the network wants to be sure about ONU's identity
  - the network wants to have means to verify that the message received and presumably created by ONU A did indeed originate from ONU A
- Access control
  - the network wants to restrict access to resources to privileged ONUs
  - requires authentication
- Confidentiality
  - keeping information secret from all but those who are authorized to see it
- Privacy
  - it is not possible to infer confidential data by passive attacks, e.g. analysis of traffic volume or destination
- Data Integrity
  - the receiver wants to be sure that the received message has not been modified

Encryption layer comparison

Requirement and importance in EPON		RS	MAC ctr w/ MIC	MAC ctr w/o MIC	IPsec
Authentication	High	Yes	Yes	No	Yes
Access control	High	Yes	Yes	No	Yes
Payload confidentiality	High	Yes	Yes	Yes	Yes
OAM confidentiality	Moderate	Yes	Yes	Yes	No
Decryption error checking	High	Yes	Yes	No	Yes
Privacy	Moderate	Yes	No	No	No
Data Integrity	Low	No	Yes	No	Yes
Protocols	High	Ethernet	Ethernet	Ethernet	IP
OLT and ONU	High	Switch	Switch	Switch	Router
Complexity	High	Low	Moderate	Low	High

Security baseline proposal (RS)

- Definition of Encryption functions to Emulation sub-layer
  - Functions are optional
  - Functions are per LLID
  - Functions have unchanging delay
  - Functions maintain frame length
  - Actions to frame: Encrypt/decrypt full frame, add/remove 3 indications [4 bits] to/from preamble
  - Static parameters from/to registers: 2 indications, encryption keys
- Out of scope of security baseline
  - Authentication
  - Key exchange
  - Re-keying
  - Cipher

Security baseline proposal (MAC control)

- Definition of Encryption functions to MAC control sub-layer
  - Functions are optional
  - Functions are per port
  - Functions have unchanging delay
  - Functions change 6 bytes frame length
  - Actions to frame: Encrypt/decrypt payload, add/remove ENC tag [2 bytes] before payload, add/remove MIC [4 bytes] after payload
  - Static parameters from/to registers: 3 indications, encryption keys
- Out of scope of security baseline
  - Authentication
  - Key exchange
  - Re-keying
  - Cipher