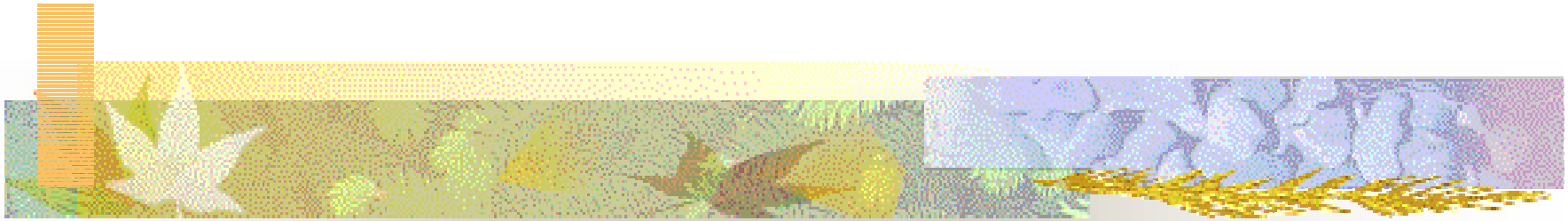
IEEE 802.3 EFM

Ethernet PON, Security Considerations



Onn Haran

onn.haran@passave.com

PASSAVE NETWORKS

Security Basics

- Demanded by customers
- Two different issues
  - Authentication
  - Privacy
- Limited to protecting the shared medium

PASSAVE NETWORKS

Authentication

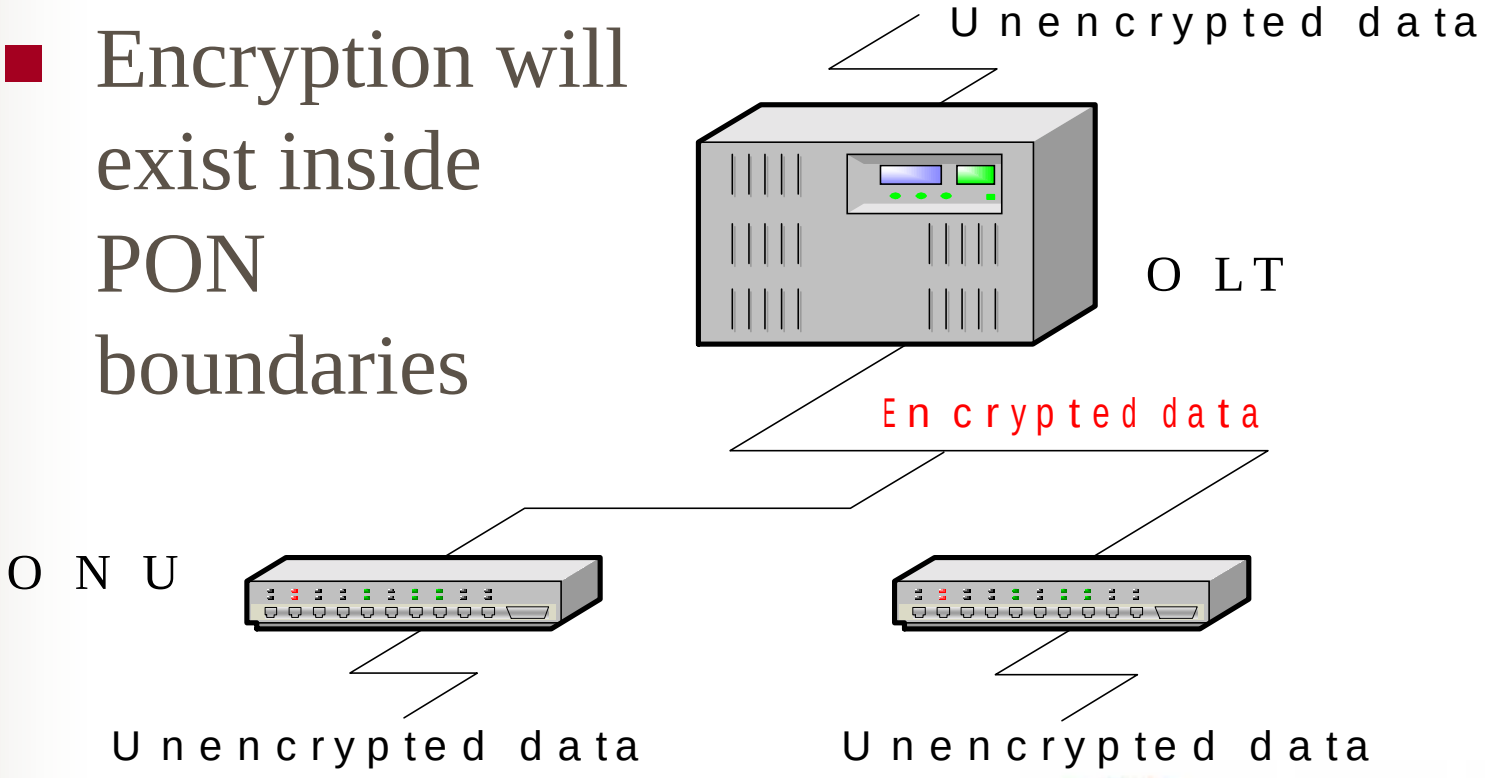
- Plug and Play
- Based on 802.1x
  - Authenticator – OLT
  - Supplicant – ONU
  - Authentication server – Need to decide on central database issues
- The medium behavior enables the use of a simplified mechanism – to be discussed

Encryption

- Downlink data should be encrypted
- Two different approaches:
  - Add MAC level encryption
  - Use higher layer mechanisms, like IPsec
- Higher layer security can't be enforced
- Other shared media protocols incorporate encryption

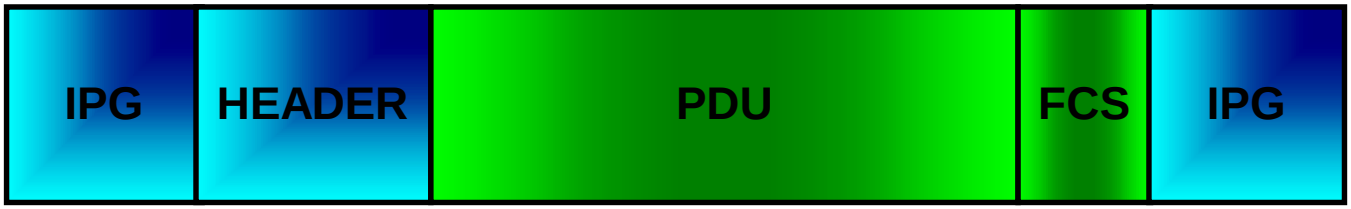
PON Domain Encryption

- Encryption will exist inside PON boundaries



Frame Format

- No new fields are needed; format is maintained
- Encryption should start following Ethernet header and end after FCS



- MAC control packets are not encrypted

PASSAVE NETWORKS

Churning

- APON uses a 24-bit key churning mechanism
- Churning is a memoryless transformation of one byte to a different byte
- Key strength is $2^{\text{key length}}$
- Drawbacks and weak points:
  - IP header
  - FCS

PASSAVE NETWORKS

DES

- DOCSIS uses 40/56 bits DES with CBC (Cipher Block Chaining)
- DES is a transformation of 8 bytes to different 8 bytes
- Having an initialization vector eliminates the weak points
- DES is fading out and not recommended for new designs

AES

- AES was designed to replace DES
- AES draft is ready. It is expected to be approved in several months
- AES is a transformation of 16 bytes to different 16 bytes
- AES supports 128, 192 and 256 bit key length

Last Block Problem

- Encryption block boundary may be dissimilar to packet boundary
- The last n bits (n < 128) will be XORed with the result of additional AES over the next-to-last block

PASSAVE NETWORKS

Key Management

- Periodic rekeying
  - APON (Churning) – every 1 second
  - DOCSIS (DES) – every 12 hours
  - EPON (128-bit AES) – every 3E17 years …
- Two challenges
  - Key distribution
  - Key synchronization

Key Distribution

- OLT has a random number generator
- OLT distributes the keys AES encrypted with a special key
- Key distribution messages are acknowledged

PASSAVE NETWORKS

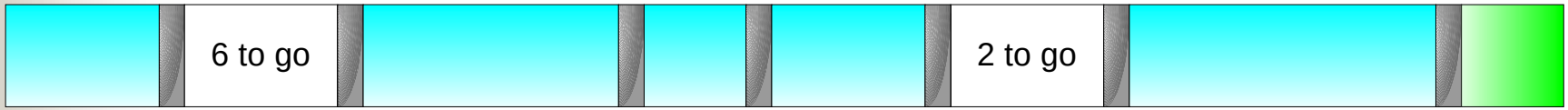
Multicast Group

- Dynamic key management for multicast group must be supported
- OLT distributes the keys using the secured unicast channel
- Removing members from a multicast group is done by rekeying all other members

PASSAVE NETWORKS

Key Synchronization

- Rekeying should not take place in the middle of a packet
- Precise time stamp is ineffective
- The OLT sends a “switch key” message with the number of packets until the switch



PASSAVE NETWORKS

Recommendations

- Add security to the MAC layer
- Maintain standard Ethernet frame format
- Adopt 802.1x
- Encryption should base on 128-bit AES
- Use key management solution as presented
- Form an “Ad-Hoc” group for security?

PASSAVE NETWORKS