Security for EPONs and Packet Size: a High-Level View

Bob Gaglianello

Providing Security for EPONs Requires the Inclusion of Information within the Packet

Any additions to a Packet run into the Ethernet (802.3) Maximum Packet size restrictions.

- Currently, the only solution for oversize packets is to fragment a packet at the transmitter and reassemble the fragments at the receiver.
- This can lead to reduced efficiency, more computational complexity and increased buffering, when compared to an EPON system that doesn’t require the need to fragment packets.

Three Techniques for Passing Security/Encryption Information

Assume all three provide the same level of "Protection"

- In Preamble
  - Limited number of bits to play with (1-2 Bytes)
  - Requires 802.3 to allow usage of preamble bits/bytes
- In a Tag / Label
  - "Limited" number of bits but many more than preamble case
  - Requires addition of tag / label fields to be standardized.
  - Requires 802.3 to increase the Max Packet Size similar to what was done with VLAN tagging of packets.
- In Payload (ipSec-like)
  - "unlimited" number of bits
  - May cause packets to be larger than Max Packet Size
  - Standardizing something "outside" the Packet Header in 802.3 is problematic at best

Conclusion

Of the three techniques, which, if any, will be palatable to 802.3

- From a P2MP viewpoint, the preferred method would be to allow a byte or two in the preamble.
  - However, is there room for the necessary security information in 1 or two bytes ??
    - Haran_P2MP_2_0702.pdf and “EPON properties for Security” discuss techniques that have the necessary small number of bits < 1-Byte).
    - More analysis is necessary to see if such techniques can provide the necessary level of security.