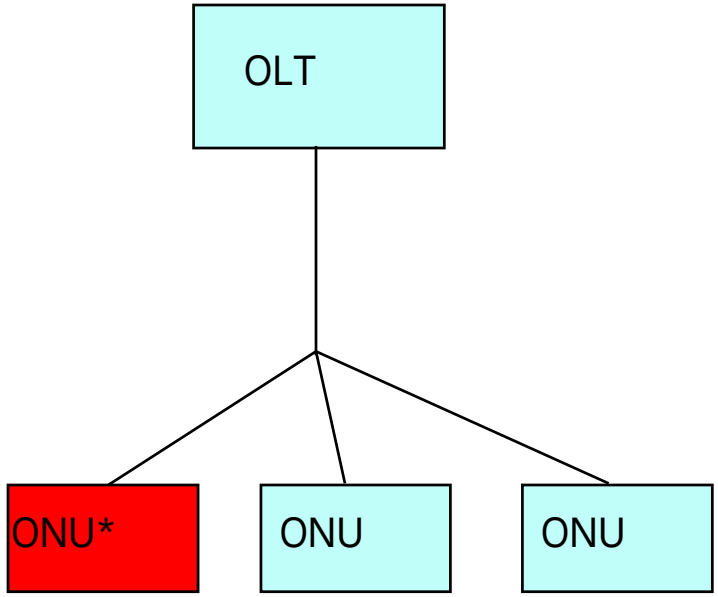
EPON threats and solutions

Antti Pietiläinen, Nokia

Requirements as proposed in July 2002 (5 authors in 3 companies)

- Provide ONU authentication
- Provide confidentiality of data and MAC addresses and control messages down and upstream
- Protect from an ONU masquerading as another ONU
- Protection against replay attack



*malicious node

Non objectives, July 2002

- Man-in-the middle considered taken care by physical protection
- Authentication of OLT not required for same reason.

EPON specials

- Encrypted frame check sequence (FCS) can be used to provide protection against replay attack and masquerading (because no man-in-the-middle)
- MAC addresses can be encrypted because LLID (logical link ID) may be used as identifier in EPON link.
- Only four bits were required to be added in preamble of each packet for security reasons and reducing to three is possible.

Proposed framework in July 2002

- IEEE802.1x would be used for authentication, access control, key exchange, and re-keying
- Key lengths, mechanisms etc. that provide high level of protection were discussed but not yet defined.
- Suitable portions would be copied from IEEE802.11i if possible.

Later proposals

- Block cipher, counter mode, and e.g. 128 bit AES was proposed. PON clock could be used for initialization vector synchronization (Haran and Hiironen, July)
- ONUs could identify themselves using temporal MAC address in register request message for protecting their identity (Hiironen, July).
- LLID will reveal identity if there is single user behind ONU. Proposal to change LLIDs secretively once a while (Hiironen, July).
- PON clock can replace replay counter (Haran, September).
- Securing registration and key exchange by creating an encrypted tunnel using public keys (Pietilainen, September).

How did it end in July 2002

- In July 2002 meeting a motion was made to enable following mechanisms to provide security: key transfer to cipher, key change indication, en/decryption indications, cipher counter synchronization.
- Passed technical vote in 802.3ah but received only about 50 % support in 802.3 plenary.

Conclusion

- By choosing a threat model where man-in-the-middle is left out and by using the proposed techniques it is possible to achieve high level of security while just utilizing about three more bits from the preamble in addition to LLID that already is part of EPON packet.
- Encrypting the whole packet gives additional protection as compared with data only encryption as in multi-hop scenarios.
- Implementation is possible with limited cost.