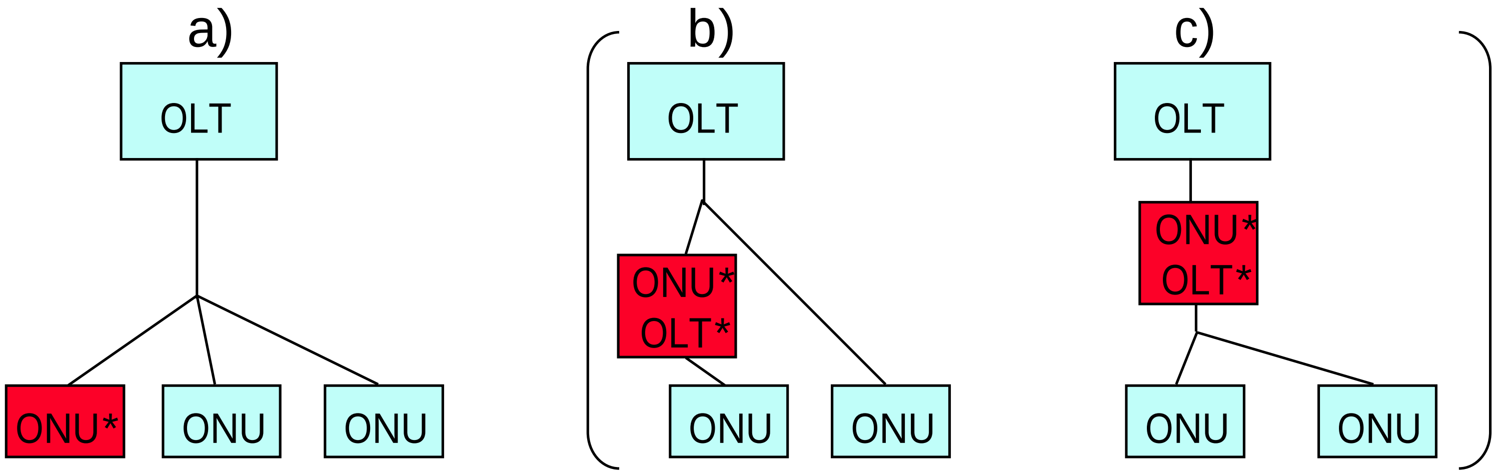
EPON subscriber access security requirements

Antti Pietiläinen, Nokia

Here only threat model a) is discussed, reasons:

- Case a) has to be considered because there eavesdropping is not only very easy but also practically impossible to get caught from.
- Subscriber networks are built in such a way that physical protection against man-in-the-middle (b and c) is assumed. In addition, a person who manages to tamper telephone lines faces a real risk of getting into trouble with the law because physical intervention leaves evidence.
- Operators are hardly considered responsible of damage caused by b) or c) if physical protection has been adequately taken care of .
- Taking care of case a) is much easier than taking care of all three. For example, b) and c) will probably increase packet length by several bytes while a) can be solved with a few bits.



*malicious node

For abiding by the law, minimum requirement

- Confidentiality has to be ensured
  - In practice this means that payload has to be encrypted when it is transmitted through an EPON link, especially downstream and preferably upstream also because eavesdropping of upstream traffic may be possible in some cases.

For being able to prevent ONUs from stealing each others bandwidth or being able to bill on per-bit or per-second basis of layer 2 service

- Unauthorized access should be prevented
  - Access control is required
  - Authentication is required
  - Message authentication is required

Suitable features

- Privacy
  - Encrypting payload ensures confidentiality but does not give high level of privacy because Ethernet MAC addresses do not change in time and, therefore, create a long-lasting link between packets and the subscribers who receive the packets. Thus, it is possible to monitor selected victims' communication habits with no risk of getting caught.
  - Unencrypted control packets would reveal upstream traffic profile of individual ONUs.
- Test signals
  - If broad encryption is utilized, it may be useful to be able to turn encryption of control packets and MAC addresses momentarily off for test purposes.
- Denial-of-service monitoring
  - It is possible to block or disturb upstream traffic. Therefore, the state machine of OLT should detect and maybe sort a few misbehavior types: general disturbance, using wrong logical link ID (LLID), etc.

Conclusion

- Encryption of downstream payload is required at minimum.
- For having better chances of obtaining general acceptance, additional effort is required for making EPON security-wise competitive against other solutions.
    - Encryption of Ethernet headers
    - Encryption of control packets
    - Access control
    - Authentication
    - Message authentication
    - Dynamically reallocated LLIDs