# Encrypting MAC addresses and MPCP messages in EPON

Antti Pietilainen, Nokia

# Encrypting MAC addresses

The following 3 pages explain why MAC addresses should be encrypted

- Ethernet is a way to provide L2 transport to connect different offices of a company. All equipment of a medium sized company may form a single L2 network even if several offices are connected.

- An eavesdropper connected to same EPON as target system can read source and destination addresses of downstream traffic of target system. Addresses reveal vendors. Furthermore, different vendors manufacture different types of equipment. Thus, the eavesdropper may find out
  - The number and vendor distribution of computers in a company
  - Acquire an estimate of which servers, firewall routers and bridges are part of the company network.
- In EPON eavesdropper has no risk of getting caught – even “respectable” people may eavesdrop.

- In literature there are claims that VLAN hopping can be generated if MAC addresses of the target system are known. In this case an eavesdropper could also cause direct harm to target system.
- Conclusion: MAC addresses simply unveil too much information if handed over to eavesdroppers and therefore should be encrypted. Otherwise, market for EPON products is severely affected.

# Encrypting control messages

- “Gate” messages describe the upstream traffic of each ONU revealing the amount of traffic, its variations with time, and reactions to  external stimuli.
- “Register” messages reveal MAC addresses of ONUs.
- It is straightforward to encrypt data, OAM, and control packets in the same way. Encryption of control messages can be turned temporarily off to measure performance of EPON and locate malfunctioning equipment.

# Conclusion

- MAC addresses and control messages should be encrypted in EPON.
- There are also claims that an eavesdropper can find out a large portion of information described above in any case using traffic analysis. However, it is probably true only to certain extent. Perhaps some additional randomization is required to achieve high level of identity protection. However, one should not give up from pursuing acceptable level of security in EPON.