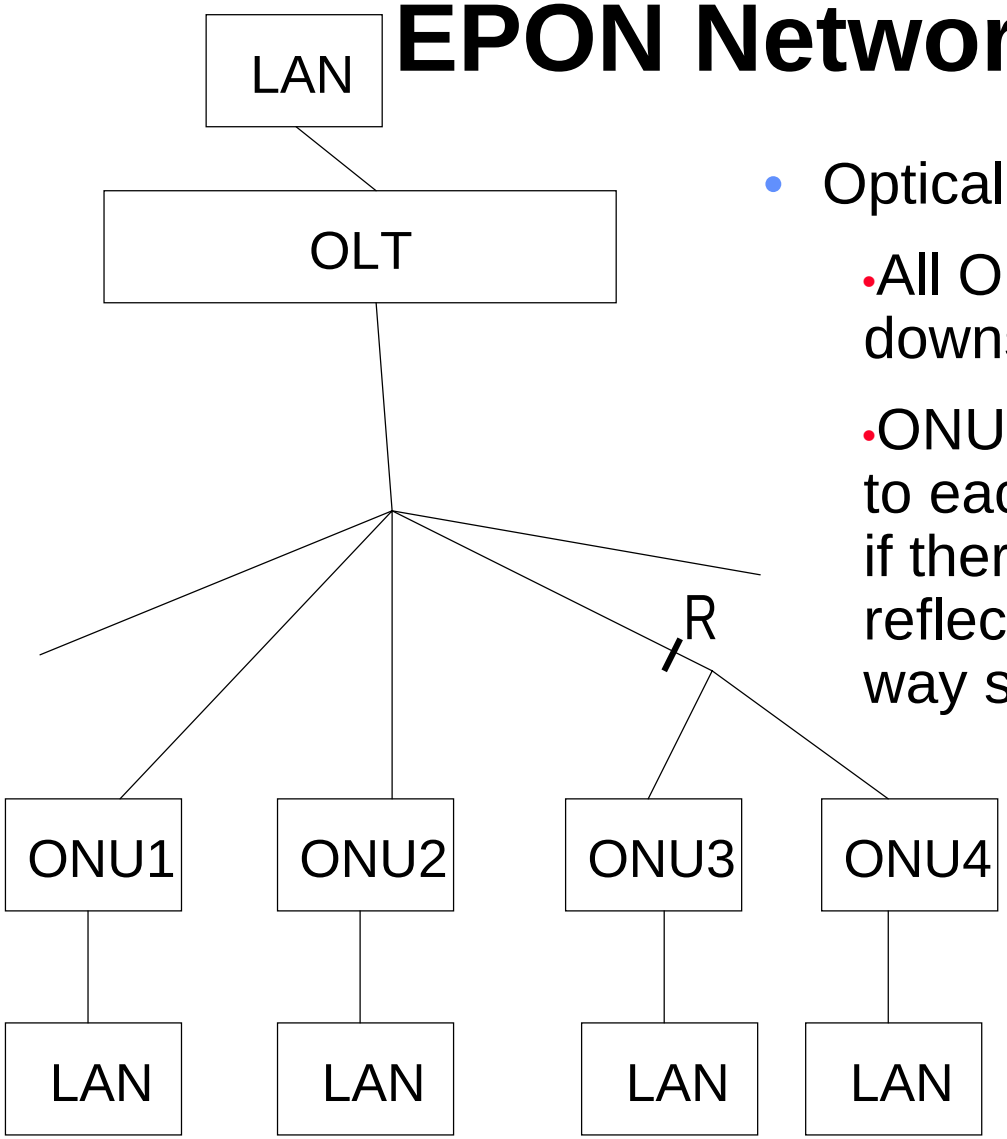
Key exchange during autodiscovery

Antti Pietiläinen, Nokia

EPON Network topology



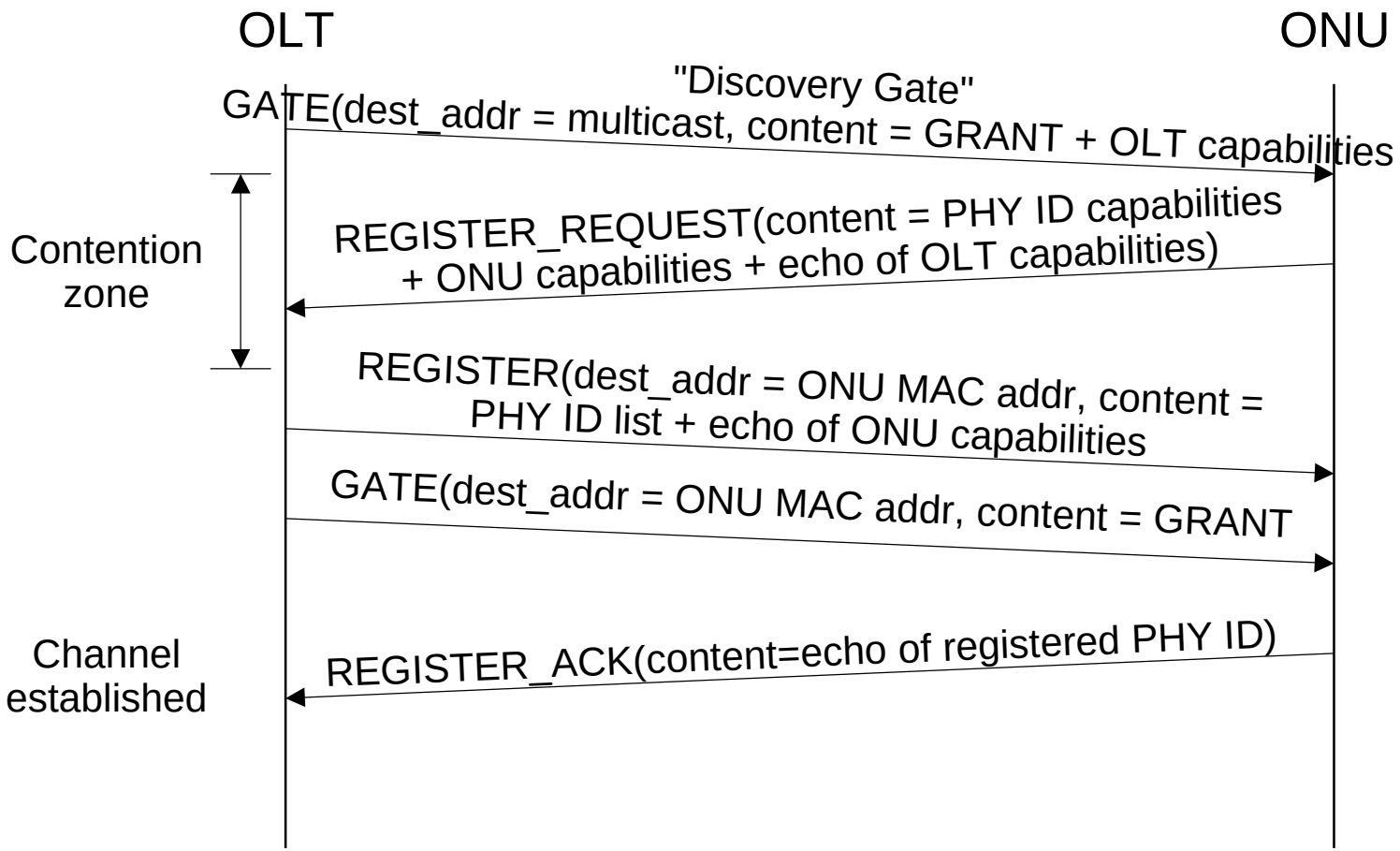
- Optical network
  - All ONUs may listen to all downstream traffic.
  - ONU3 and ONU 4 may listen to each others upstream traffic if there is large enough reflection at point R above a 2-way split.

EPON = Ethernet passive optical network

OLT = optical line terminal

ONU = optical network unit (in or near user residence)

ONU auto-discovery as of May 2002



Ref. Gaglianello_1_0502.pdf

Motivation

- Confidentiality and privacy over the link are most important. Authentication could be carried out after the encrypted channel is present.
- Very little sensitive information is revealed if encryption is started immediately -> key exchange should be made part of registration process.
- If keys are random numbers that do not carry authentication information, they can be generated below MAC in EPON chip hardware. The solution would be internal to 802.3 EPON and would not require interplay between 802 standards. External cryptographic standards could be used.
- Keys would not have to be passed across network layers.
- 802.1x could be used for authentication after the encrypted link is up. The 802.1x protocol could be carried out without special requirements from EPON.

ONU auto-discovery w. key exchange and encryption. 802.1x port authentication protocol is used for authentication.