

Security in MPCP auto-discovery

Olli-Pekka Hiironen, Nokia

Security threats in auto-discovery

- Denial of service

- The attacker may try to register using other ONU's registered MAC address. System should know which REGISTER_REQUEST to accept
 - 1) ONU1 has registered using his fixed MAC address. Connection fails and ONU1 sends new REGISTER_REQUEST.
⇒ OLT **should accept** registration request and remove the old connection.
 - 2) ONU1 has registered using his fixed MAC address. Attacker sees the MAC address from REGISTER message and sends REGISTER_REQUEST using that MAC address.
⇒ OLT **should not accept** the registration request. Conflict with 1.
 - 3) Attacker have registered using ONU1's MAC address. ONU1 sends REGISTER_REQUEST using his fixed MAC address.
⇒ OLT **should accept** the registration request and remove the old connection. Conflict with 2.

⇒ **Different temporal MAC address should be used each time in auto-discovery and auto-discovery should be ratified by authentication**

Security threats in auto-discovery

- Privacy

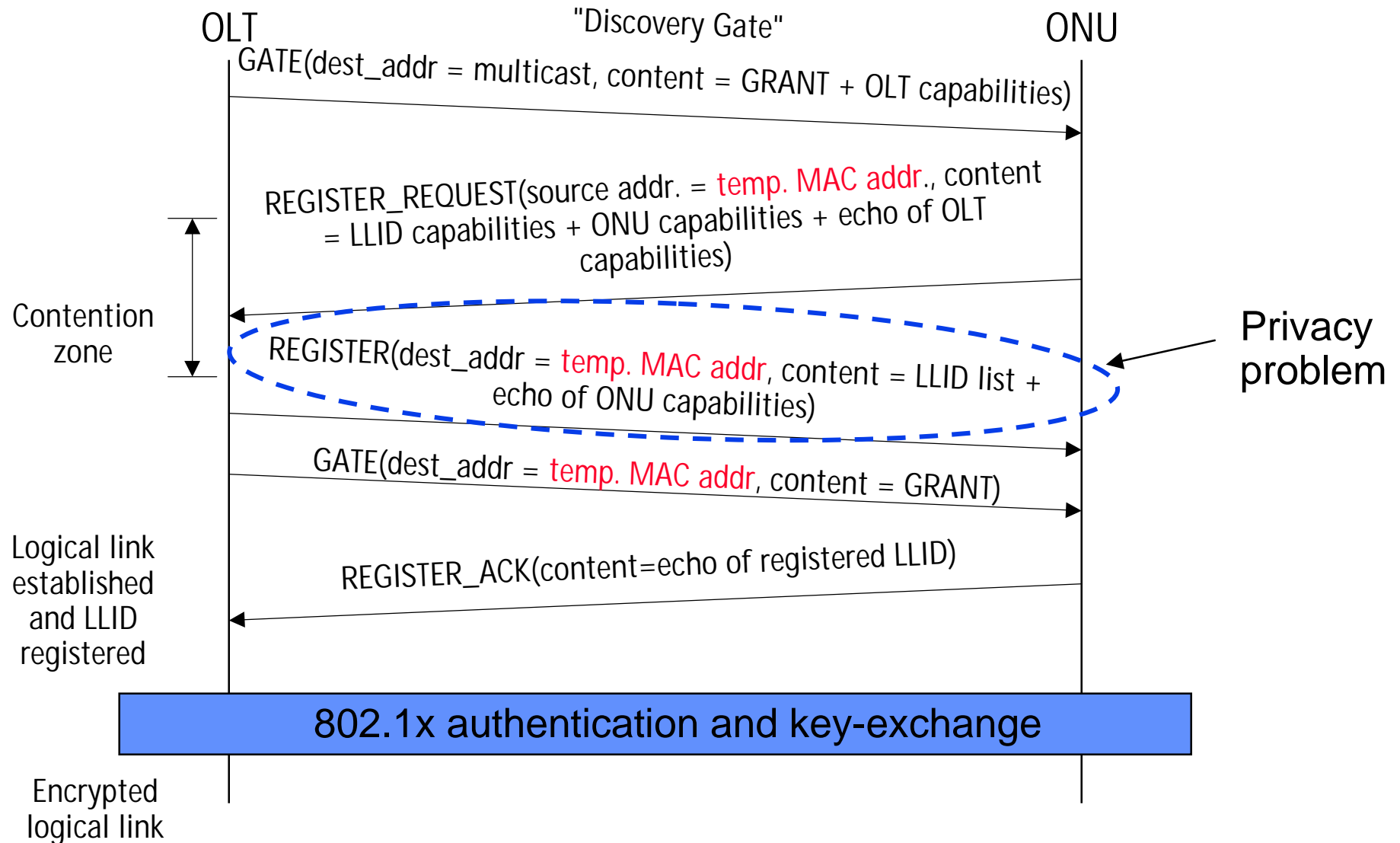
- ONU MAC address is visible in the REGISTER-message. The knowledge of neighbors MAC address can be seen as a privacy violation.

⇒ **Temporal MAC addresses should be used in MPCP auto-discovery instead of ONU MAC addresses**

- Identity of LLIDs is coupled with ONU in the REGISTER-message. LLID identity is equal to user identity if there is only one user behind LLID
- Traffic analyzing is possible with identified LLIDs. The knowledge of the amount and type of traffic to neighbors (or to neighbor company) is a privacy problem

⇒ **The identity of LLID should be hidden by changing the LLID secretively once in a while**

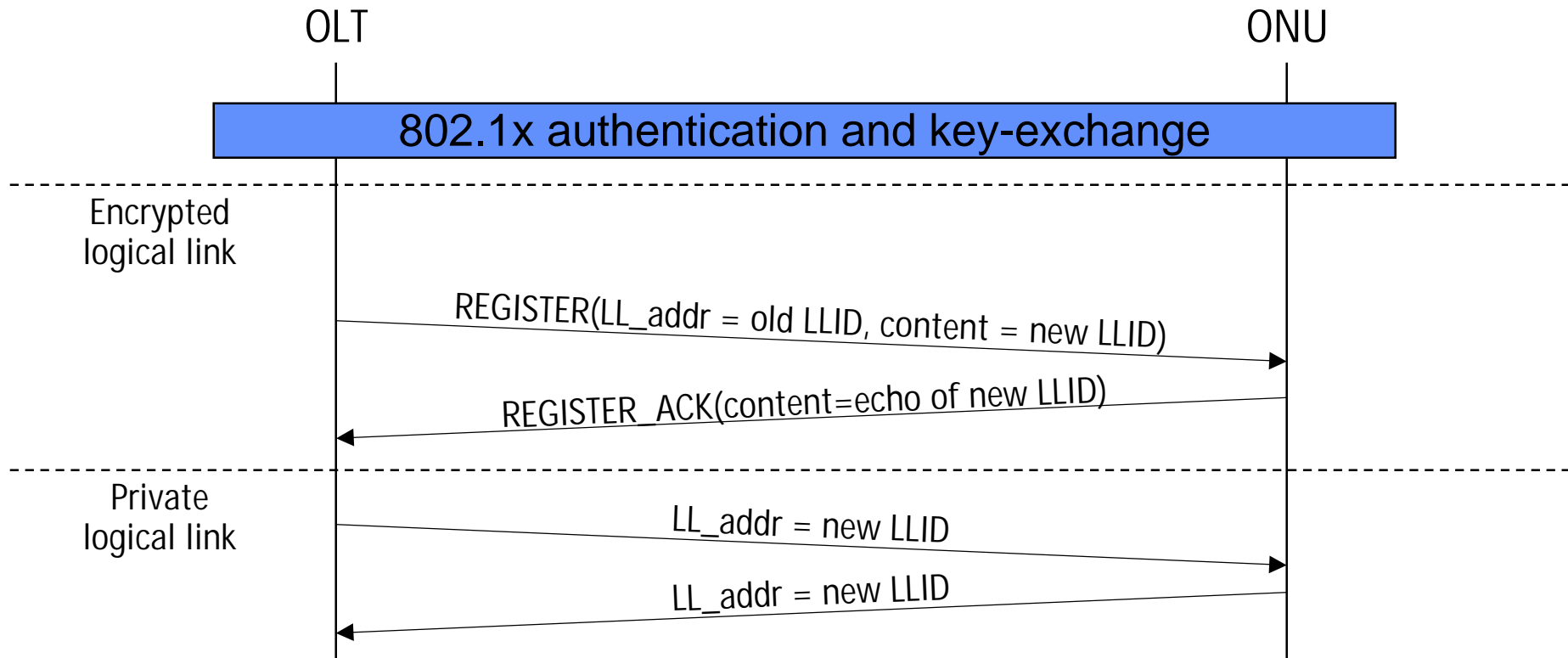
Secure auto-discovery



Secure auto-discovery

- Temporal MAC address is used in auto-discovery
- ONU will use different temporal MAC address in each REGISTER_REQUEST attempt
- If the temporal MAC address is already in use, situation is same as in contention; REGISTER_REQUEST will be ignored and ONU will send new REGISTER_REQUEST using different temp. MAC address
- If two ONUs are using the same temporal MAC address in the same discovery window, then both should be ignored
- Successful authentication will ratify the auto-discovery
- Temporal MAC address is used only in the auto-discovery, it is not used afterwards
- Other MAC addresses will be learned through the LLID ports after logical links are established

LLID identity hiding



- Old, identified LLID will be changes through encrypted channel to new, unidentifiable LLID
- New LLID will be taken into use after REGISTER_ACK

Motion 1

- Use of different temporal MAC addresses in each MPCP auto-discovery should be allowed for preventing privacy and denial of service attacks.

Motion 2

- Allow the use of REGISTER-message for changing LLID dynamically to give means to prevent privacy attacks.