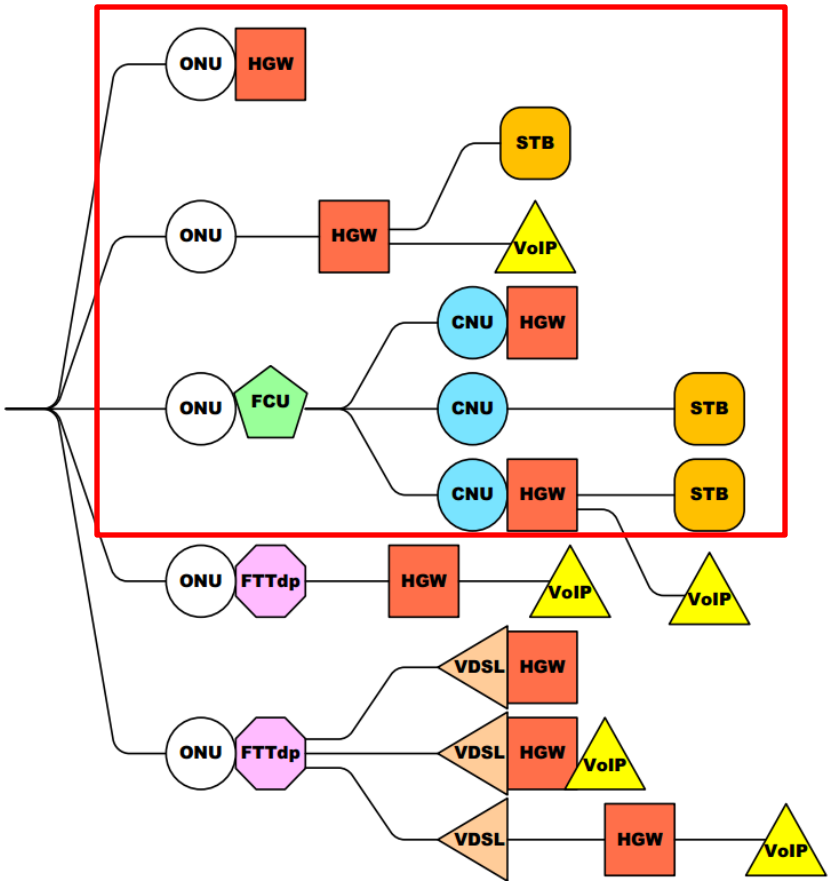
UNIVERSAL MANAGEMENT TUNNEL (UMT) REQUIREMENTS

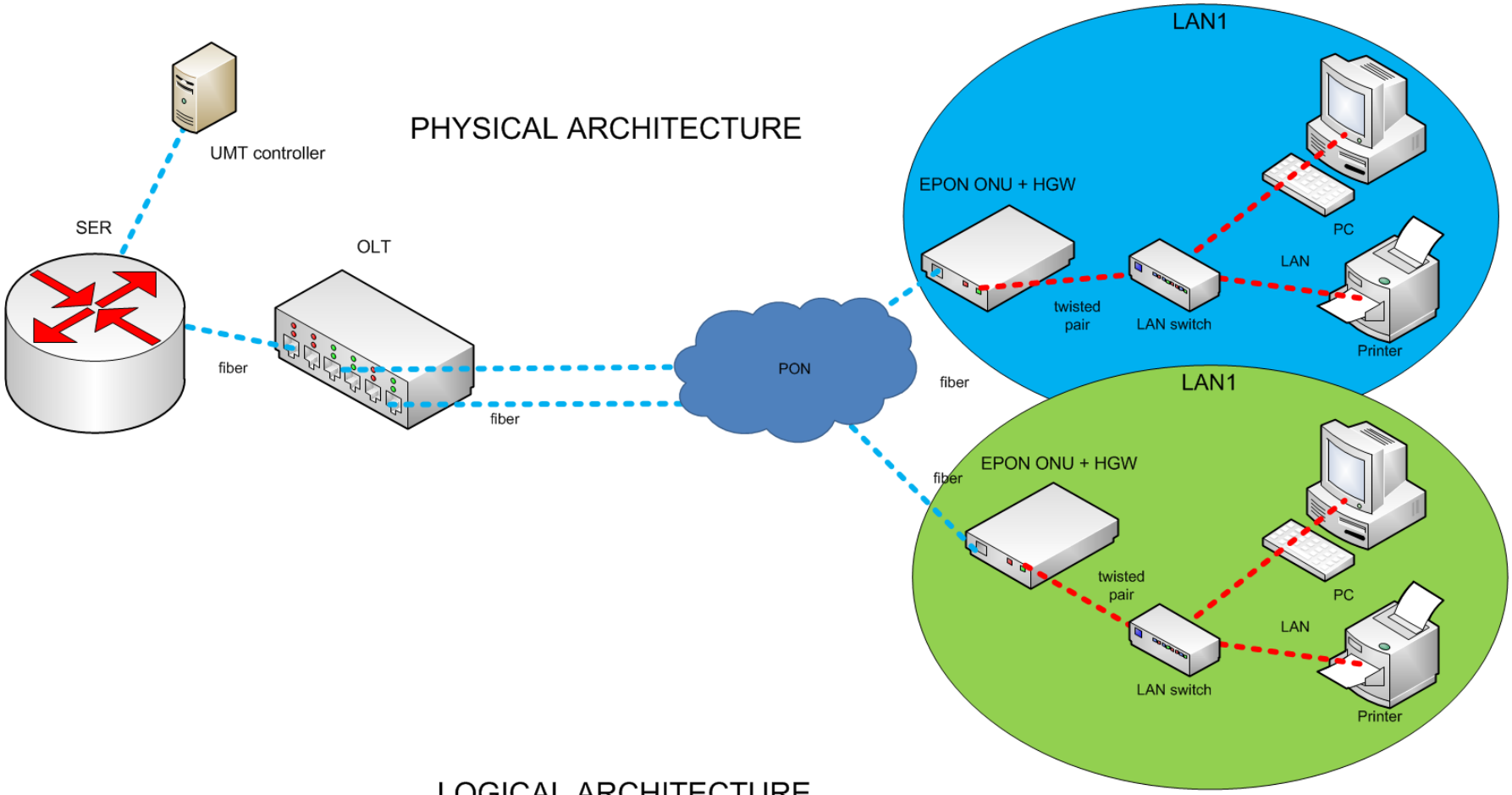
CONTACT:
MAREK HAJDUCZENIA
NETWORK ARCHITECT, PRINCIPAL ENGINEER
OFFICE +1-813-295-5644
CELL +1-813-465-0669
EMAIL: MAREK.HAJDUCZENIA@MYBRIGHTHOUSE.COM

UMT Applications

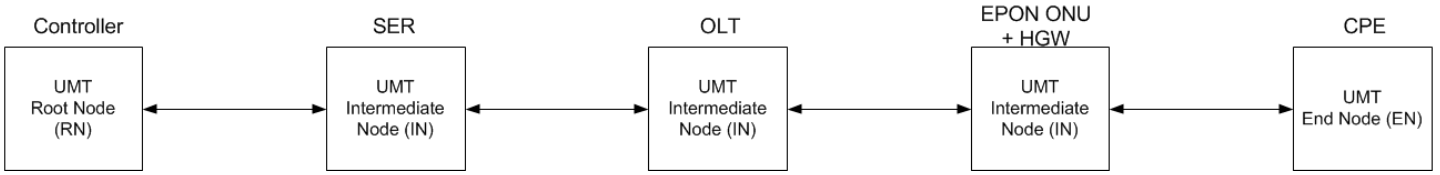
- Primary interest in following UMT applications:
  - OLT ⇔ FCU ⇔ CNU
  - OLT ⇔ ONU ⇔ LAN
  - SER ⇔ field OLT ⇔ ONU ⇔ LAN
    - Field OLT = a hardened OLT with direct uplink to an edge router
- Ability to classify on UMT traffic at ONU is very important
  - Management traffic discounted from user bandwidth profile and carried over a dedicated service flow
  - Even more important in usage-based billing models



Target Architecture (1)



LOGICAL ARCHITECTURE



Target Architecture (2)

- Each node is designated one of two functions:
  - Intermediate Node (IN): forwards UMT PDUs between ports but does not participate otherwise in UMT exchange.
  - IN is authenticated to Root Node (RN) via a series of other INs (chain of trust).
  - End Node (EN): terminates UMT domain and consumes UMT PDUs.
  - EN is authenticated to RN via a series of INs (chain of trust).
- RN announces its presence to all connected INs and ENs
  - Periodic beacon sent to all UMT ports
    - Maximum frequency low to avoid DoS-like behavior
  - INs and ENs only respond to beacons when hunting for new RN (primary or secondary). Other beacons are ignored.
  - INs and ENs may need to change selected primary RN over time based on some metrics (e.g., distance, reliability, etc.)

Requirements for UMT (1)

- Ability to traverse L3+ NAT devices
  - Required for managing LAN devices across OLT and ONU
- Data rate / throughput
  - Configurable on all intermediate nodes during initial configuration / UMT capability negotiation
  - Fixed data rate / throughput should be avoided – there are different deployment models, application scenarios, etc.
- Latency
  - Should be not worse than latency for customer traffic
- Security
  - Mutual authentication between each intermediate node and root
  - Mutual authentication between end node and root
  - Encryption between end node and root

Requirements for UMT (2)

- Support (minimum) for following protocols
  - OAM (Clause 57) with SIEPON / DPoE extensions
  - SNMP
  - TR-069
- Reliability
  - Support for multi-root homing, i.e., when primary root node goes offline / fails to respond, end node switches to secondary root
  - Support for a hierarchy of secondary roots (multiple secondary roots, ordered against their distance from end node)
  - TCP-like session-based exchange with delivery guarantees for UMT session traffic (?)

THANKS !