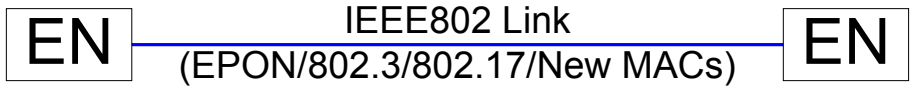
Link Security Scenarios

Ali Abaye
Charles Cook
Norm Finn
Russ Housley
Marcus Leech
Mahalingam Mani
Bob Moskowitz
Dave Nelson
Antti Pietilainen
Allyn Romanow
Dan Romascanu
Dolors Sala
Mick Seaman
Dennis Volpano
Glen Zorn

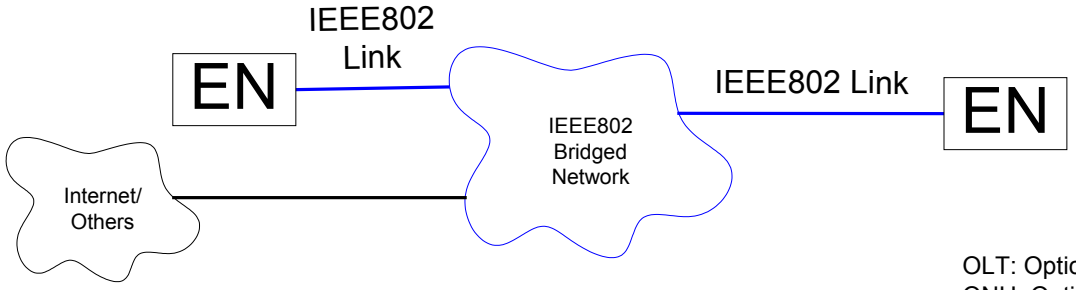
Business Scenarios

B1) EPON link scenario - Required (imminent need)

B2) Extension to other IEEE802 links/MACs - Required



B3) Layer 2 Network - Required



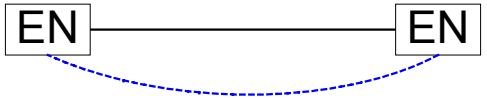
OLT: Optical Line Terminal (CO side)
ONU: Optical Network Unit (Client side)
EN: End Network Point
In blue: Scope of secure communication

Business Applications

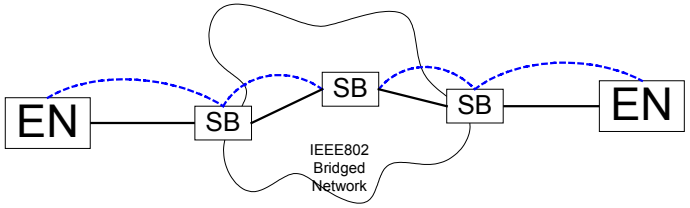
- **Scenario B1: EPON Security**
  - FTTH/FTTB (provider network)
- **Scenario B2: IEEE 802 Link Security**
  - 802.3ah copper (DSL) network (copper is easy to tap)
  - Any 802 Enterprise network (networking devices in secure locations)
- **Scenario B3: Secure Bridged Networks**
  - Layer 2 provider networks (networking devices are not in secure locations)

Trust Scenarios

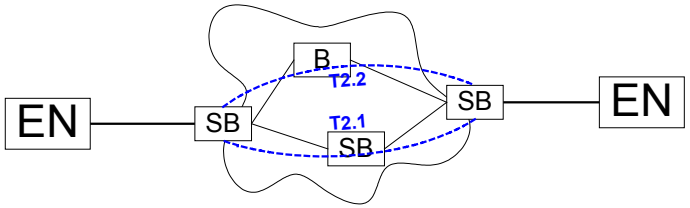
T0) Secure link communication - Required



T1) Single-hop secure bridged communication - Required

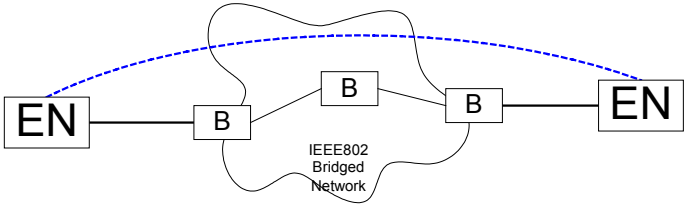


T2) Multi-hop secure bridged communication - Required



T2.1) Adjacent case - First
T2.2) Non-adjacent case - Later

T3) Layer 2 end-to-end secure communication - Nice to have



EN: End Network Point
SB: Security-aware Bridge
In black-solid: Physical communication
In blue-dotted: Logical secure communication

Scenario T0: Secure Link

- **Definition:**
  - A single link is secured
  - Security mechanism addresses MAC vulnerabilities
- **Requirements/Assumptions:**
  - Communication is “secure” on the wire only
  - Network device must be in trusted buildings for a complete secure architecture
  - MACs required to support: all 802.3 topologies
- **Business Applications:**
  - EPON scenario where ONU is inside home or business and OLT in CO building

Scenario T1: Single-hop Secure Bridged Network

- **Definition:**
  - Securing a bridged network by securing each link independently
  - Security scope is the MAC and packet is forwarded in clear to bridge level
  - This case is a cascade of several T0 Scenarios (each one can potentially operate with a different MAC)

- **Requirements/Assumptions:**
  - Still, communication is “secure” on the wire but not in the network devices
  - Network device must be in trusted buildings for a complete secure architecture
  - It does not effect the bridge functionality but it does require an extended (secure) MAC in every port of the bridge (infrastructure “upgrade”)
  - Links already secured by other means can continue using the existing security mechanism (examples: 802.11, 802.16, 802.15 links)

- **Business Applications:**
  - Same as Scenario T0
  - Enterprise Layer 2 networks (networking devices are in trusted buildings)

Scenario T2: Multi-hop Secure Bridged Network

- **Definition**
  - Securing a bridged network by transparently bridging encrypted packets
  - Security is only applied at the entrance of the packet (either by the end station or “close”bridge) or trusted points
  - Can use existing bridged networks to transport the secured packets
- **Requirements/Assumptions**
  - No security assumptions on network infrastructure
  - Requires a transparent secure data encryption (SDE) protocol
  - Needs some awareness of security in the network:
    - Every device (case T2.1): any bridge can take the function. Simpler at bridge level but more “upgrades”
    - Few devices (case T2.2): Requires a discovery protocol to replace a security-aware bridged for another security-aware bridged during topology changes
  - Should operate with any IEEE802 MAC
- **Business Applications**
  - Provider Access/MAN environments

Scenario T3: End-to-end Secure Layer 2 Communication

- **Definition:**
  - Security is done station to station
  - Network is not aware of security

- **Requirements/Assumptions**
  - Stations (or end system) must support security mechanism
  - SDE protocol must be transparent
  - This is a “simple” case of multi-hop secure bridged network

Functional Scenarios

Classification of scenarios based on functionality needed:

- **F1: Link Protection (High Priority for 802.3 networks)**
  - Addresses scenarios T0 and T1
- **F2: Adjacent bridge-to-bridge (High Priority)**
  - Addresses trust scenario T2 with infrastructure T2.1
- **F3: Non-adjacent bridge-to-bridge (Medium/Low Priority)**
  - Addresses trust scenario T2 with infrastructure T2.2