***Figura 1 (Correzione: 802.15.4, non ZigBee)***

**Considerazioni e informazioni varie sui protocolli dell’ambito IoT**

* Bluetooth non è nato per il modo IoT. Oggi c’è una concorrenza “imprevista” con ZigBee per quanto riguarda alcuni ambiti.
* Bluetooth non è in grado di connettere molti dispositivi assieme.
* Prima di studiare uno standard, chiedersi quali layer copre.

**Perché ZigBee, pur essendo “costruito” sopra IEEE 802.15.4 [rif. F1], rende possibile comunicare tra lunghe distanze?**

Perché supporta la comunicazione multi-hop e alcuni end devices Zigbee possono funzionare anche come router.

**Principali vantaggi 5G rispetto al 4G**

* Maggiore densità di connessione (campo dell’IoT).
* Maggiore mobilità e minore latenza (guida autonoma, smart surgery).
* Maggiore largezza di banda (Download/streaming contenuti multimediali).

**Principali protocolli di livello applicativo**

ZigBee, Bluetooth, MQTT, CoAP.

**PROBLEMA DELL’INTEROPERABILITÀ**

**Vertical silos e vendor lock-in, possibile soluzione**

Il vertical silos è una soluzione creata “da zero”, quindi progettata dal livello fisico a quello applicativo.

Il vendor lock-in è la strategia di marketing che consiste nel legare il cliente ai prodotti dell’azienda, di fatto legandolo al vertical silos creato dalla stessa.

Ma ciò introduce problemi di interoperabilità tra i vari dispositivi. La soluzione è introdurre standard.

**Perché un’azienda avrebbe interesse a promuovere lo sviluppo di standard ed utilizzarli se poi non può più sfruttare appieno il vendor lock-in (secondo la definizione data nella domanda precedente)?**

Perché i costi per sviluppare buone soluzioni proprietarie per tutti i livelli sono decisamente alti e perché può comunque mantenere la propria esclusività e “legare” il cliente sfruttando altri aspetti, come le applicazioni, i servizi e i dispositivi stessi.

**Coopetition**

Cooperazione di aziende “rivali” per quanto riguarda lo sviluppo di standard, competizione sugli aspetti appena menzionati.

**Il problema dell’interoperabilità viene così risolto completamente?**

No, è spostato ai livelli più alti, in particolare a quello applicativo. Esistono diversi standard molto utilizzati (ZigBee, Bluetooth, MQTT, CoAP, ligtweightM2M).

**Quale è la soluzione a questo ulteriore problema?**

L’introduzione di gateway di livello applicativo.

**Gateway**

In [informatica](https://it.wikipedia.org/wiki/Informatica) e [telecomunicazioni](https://it.wikipedia.org/wiki/Telecomunicazione), in particolare nelle [reti informatiche](https://it.wikipedia.org/wiki/Rete_informatica), un gateway (dall'[inglese](https://it.wikipedia.org/wiki/Lingua_inglese) cancello, passaggio) è un [dispositivo di rete](https://it.wikipedia.org/wiki/Dispositivo_di_rete) che collega due [reti informatiche](https://it.wikipedia.org/wiki/Reti_informatiche) di tipo diverso operando sia al [livello di rete](https://it.wikipedia.org/wiki/Livello_di_rete) che ai livelli superiori, del modello [ISO/OSI](https://it.wikipedia.org/wiki/ISO/OSI), con lo scopo principale di veicolare i [pacchetti](https://it.wikipedia.org/wiki/Pacchetto_(reti)) di rete all'esterno di una [rete](https://it.wikipedia.org/wiki/Rete_di_telecomunicazioni) locale ([LAN](https://it.wikipedia.org/wiki/Local_Area_Network)).

**Integration gateway**

Gateway che unisce più sottoreti locali (ognuna con il proprio gateway e potenzialmente che utilizza un protocollo diverso) e che si occupa delle relative traduzioni di protocollo. (?)

**Quali sono i vari tipi di gateway, in quali si collocano gli integration gateways (\*)? (gr.sl. 1.1, da pag. 43, sl. 87). Figura del Tipo D nella domanda 1.**

Tipo A: dispositivi dello stesso venditore e che utilizzano lo stesso protocollo (tipico caso vertical silos).

Tipo B: dispositivi di diversi venditori e che utilizzano lo stesso protocollo.

*In A e B il gateway (service gateway) serve semplicemente a connettere la rete locale con il resto del mondo, effettuando inoltre una traduzione per rendere i dispositivi “accessibili” dall’esterno tramite un protocollo tipico di Internet.*

Tipo C\*: integration gateway che unisce n sottoreti differenti, ognuna che utilizza un diverso protocollo, si occupa di tutti i mapping tra un protocollo e un altro. Escluso il mapping con l’esterno, abbiamo quindi internamente (n\*n-1) mapping.

Tipo C/II\*: visivamente simile alla C, ma l’integration gateway “decide” il protocollo che gli altri dispositivi devono utilizzare, esponendo un’interfaccia. È il caso di Alexa o di Google Home. Ciò a causa delle “potenze di mercato” asimmetriche (ragionamento esteso a 1h5’ circa). Neanche qui il problema dell’interoperabilità scompare, ma è spostato ad un livello più alto (es. competizione tra Google ed Amazon).

Tipo D\*: integration gateway distribuito tra più dispositivi, i quali utilizzano lo stesso protocollo. Esso realizza un mapping tra ogni protocollo interno ed il proprio. Abbiamo in questo caso (esclusi quelli con l’esterno) n mapping, detto n il numero delle sottoreti.

**Perché (considerando la figura del tipo D) n e non 1?**

Perché per ragioni di semplicità e adattabilità conviene creare gli integration gateways interconnessi tutti uguali.

**Ragionamento interessante al minuto 59 (cosa significa utilizzare protocolli diversi, es. discovery protocol)**

La traduzione di un protocollo non comporta solo adattare il formato del pacchetto da un protocollo all’altro, ma significa anche mappare un comportamento di un protocollo a quello (potenzialmente del tutto diverso) di un altro protocollo.

**Svolgere l’esercizio: gr.sl. 1.1, pag. 44, sl. 90; si intendono mapping bidirezionali**

(vedere la risposta alla domanda sui tipi di gateway) Soluzione: [(n\*(n-1))/2, n]

**A cosa è dovuto il problema della sicurezza in ambito IoT?**

Dal fatto di avere reti e disp.i (con e senza vincoli) molto eterogenei tra di loro. Inoltre, per ragioni commerciali i dispositivi sono progettati concentrandosi solo sulle funzionalità e non sulla sicurezza. Possibili rischi: injection di dati falsi, controllo attuatori.

**Problema end devices con vincoli**

Anche in presenza di soluzioni a questo problema, resta il problema degli end devices con vincoli (ad esempio possono non essere in grado di effettuare mutua autenticazione).

**Come si è (in parte) risolto il problema**

La IUT-T (unione internazionale delle telecomunicazioni) ha prodotto uno standard di raccomandazioni. Una delle più importanti è quella di provvedere mutua autenticazione (a livello applicativo, non solo di rete) tra il gateway e l’end device, in particolare quando un disp.o si aggiunge alla rete. Un’altra è il controllo di sicurezza, ovvero la trasparenza e il salvataggio di tutti gli accessi e i tentativi di accesso ai dati.

**Perché la maggior parte di queste raccomandazioni riguardano il gateway?**

Perché di solito i disp.i IoT non sono direttamente esposti alla rete e perché generalmente il gateway ha la capacità computazionale adatta per implementarle.

**Perché bisogna implementare mutua autenticazione anche a livello applicativo?**

Perché su un disp.o possono esserci più applicazioni e i due aspetti sono in parte indipendenti.