# Edge Computing

Iot disrupt the cloud…

The IoT has some need that the cloud cannot satisfy

* Real Time: often decision are made in milliseconds, to late for cloud connections
* Connectivity: mobile networks are often spotty and cannot guarantee connectivity to the cloud
* Data Volume, the amount of data generated by sensors can be huge, which can block a wide area communication channel.

The edge will provide compute power and storage in the space between the device and the cloud, includes:

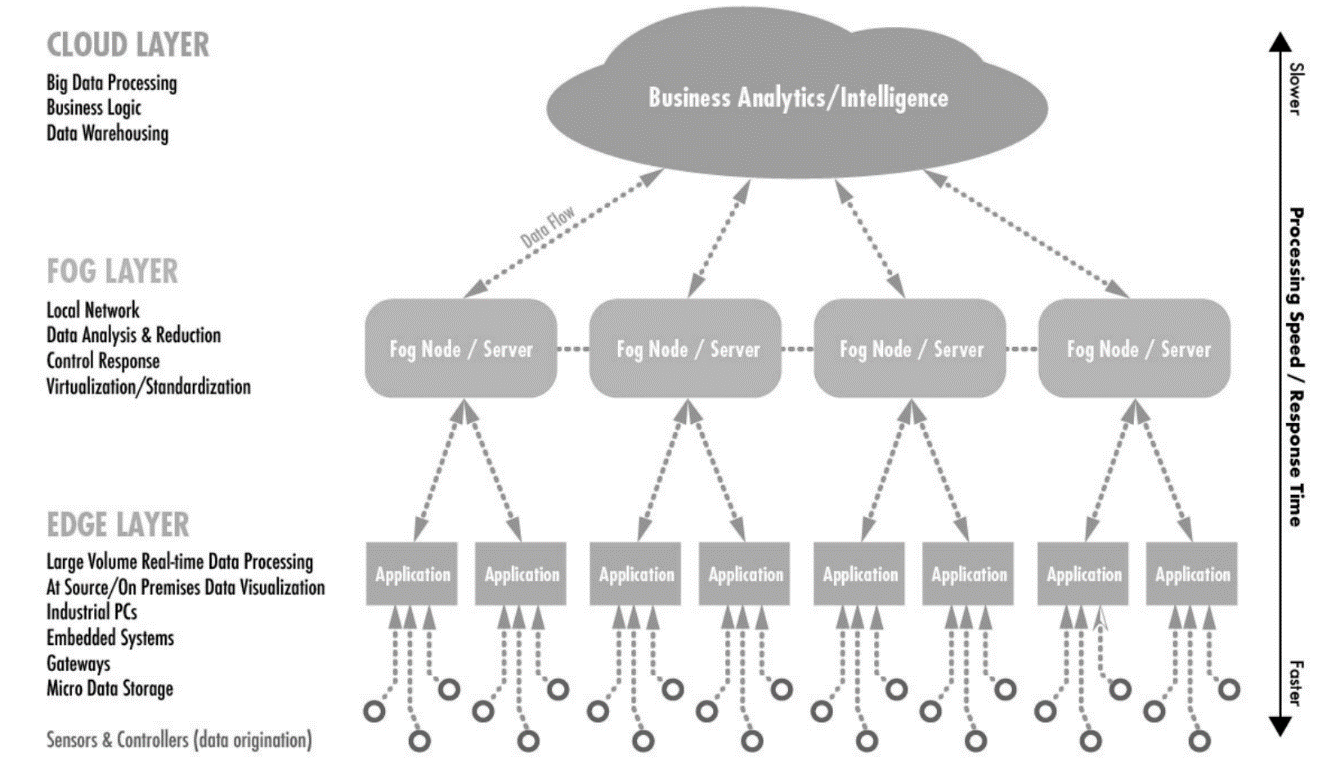
* IoT Gateways
* Routers
* Micro data centres on the Edge and on mobile network base station

Thid model have:

* Autonomous, local decision making.
* Peer to peer networking.
* Edge Networking
* Distributed queries (data in device and cloud)
* Distributed data management (decide which data store and for how long)
* Self learning algorithms

**Edge/Fog computing**

Brings computation, storage and networking resources at the edge of the access network in order to enable:

* Real time data processing
* Minimal latency
* Best QoS/Expierience
* Independence from internet connectivity for operation
* Flexible networking, security and privacy

The key difference between the two lies in **where** the location of **intelligence** and compute **power is placed**:

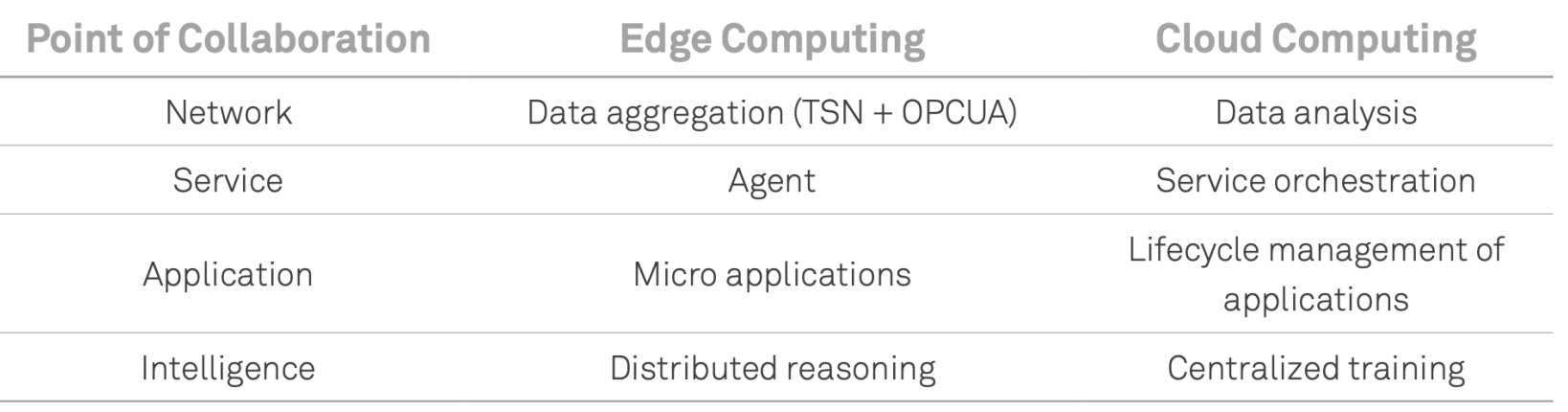
**Fog computing** environment place it at the Local Area Network (**LAN**)

**Edge Computing** places intelligence and processing power **in devices** such as smart object and embedded automation controllers.

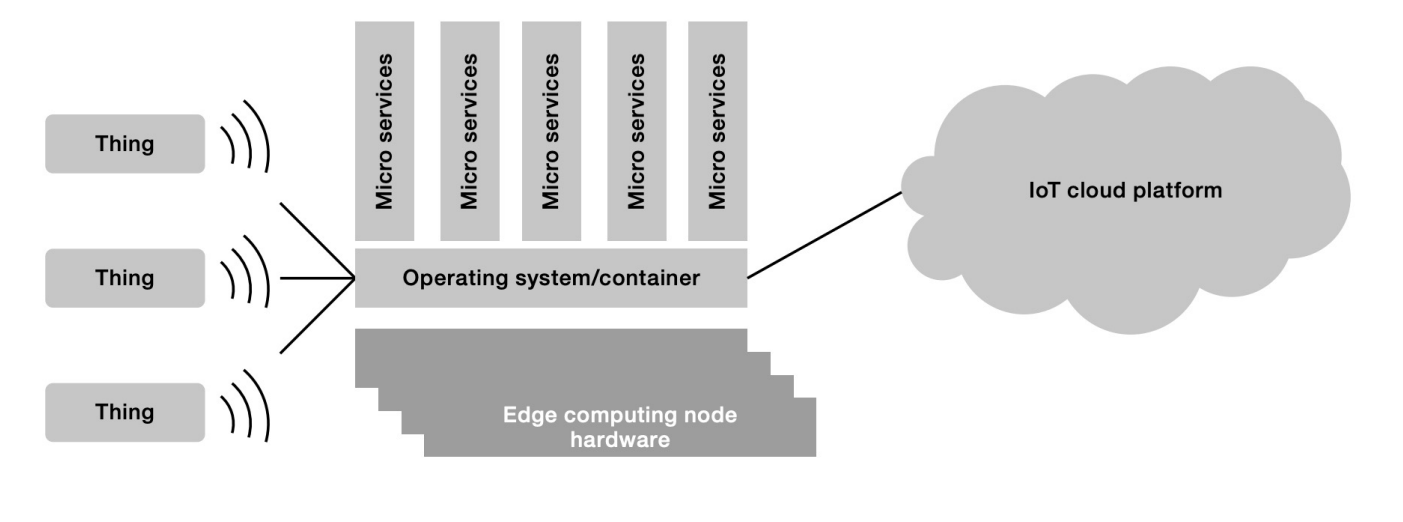
**Collaboration between edge and cloud:**

Cloud computing is suitable for non-real-time low latency and critical tasks, long-period data and business decision-making scenarios.

The edge covers the real rime scenario, low latency, short period data and local decision making also in case of offline context.



Containers provide security through isolation; they also serve as deployment units that simplify lifecycle management through less interdependency and complexity.



**The IoT Gateway** purpose is to be near the data source in the way which is easy to process.

Os Running on IoT gateways is usually general purpose Os such a s Linux

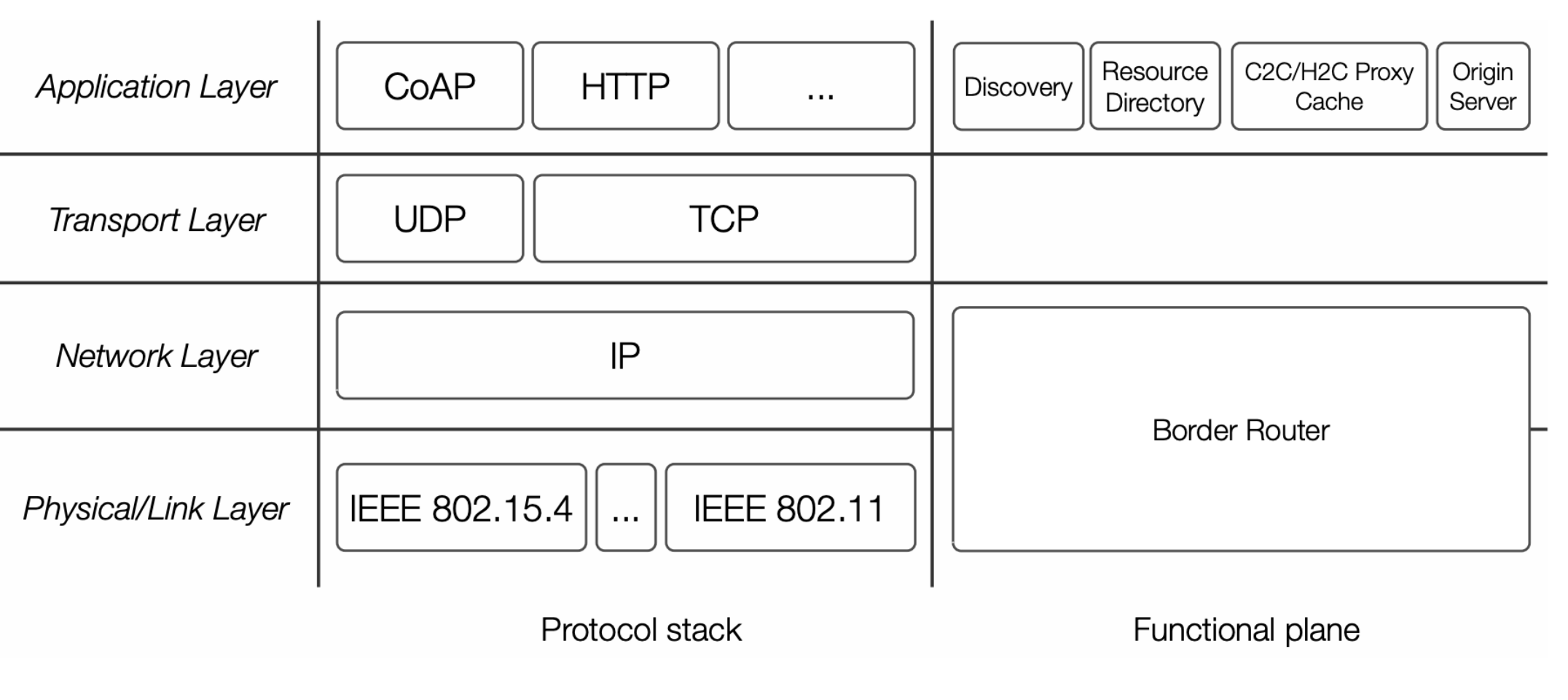
**The IoT Hub**

Is a Fog node placed at the edge of multiple physical networks with the goal of creating an IP-based IoT network to be used as an infrastructure for the deployment of WoT application.

Do not present limitation as computational power and available memory

Play a fundamental role by implementing the following functions at different layers of the protocol stack:

* Border Router
* Service and Resource Discovery
* Resource Directory (RD)
* Origin Server
* C2C Proxy (CoAP to CoAP)
* H2C Proxy (HTPP to CoAP)
* Cache

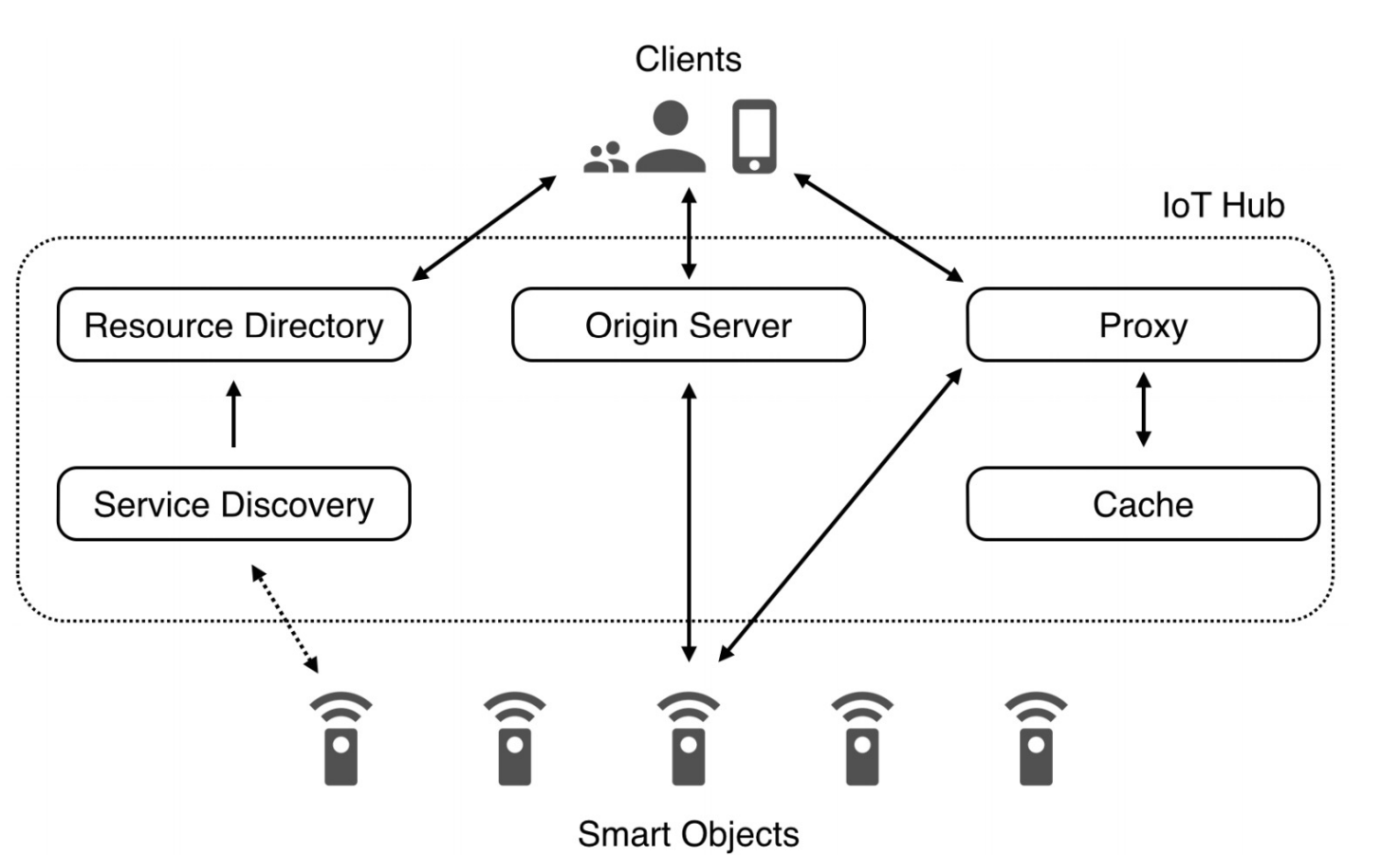


**Border router:**

The hub is the gateway/bridge between one or more constrained networks.

* Provides a intra.network IP routing
* Single addressing space for multiple network

**Layer Functions:**

****

**Service and Resource Discovery**

Aim at retrieving the scheme, IP address, and port at which a smart object endpoint is reachable.

* Use of DNS service discovery
* The use of Nmap
* Other mechanism

Once endpoint have been discovered they can be requested to retrieve the list of resources

**Resource directory**

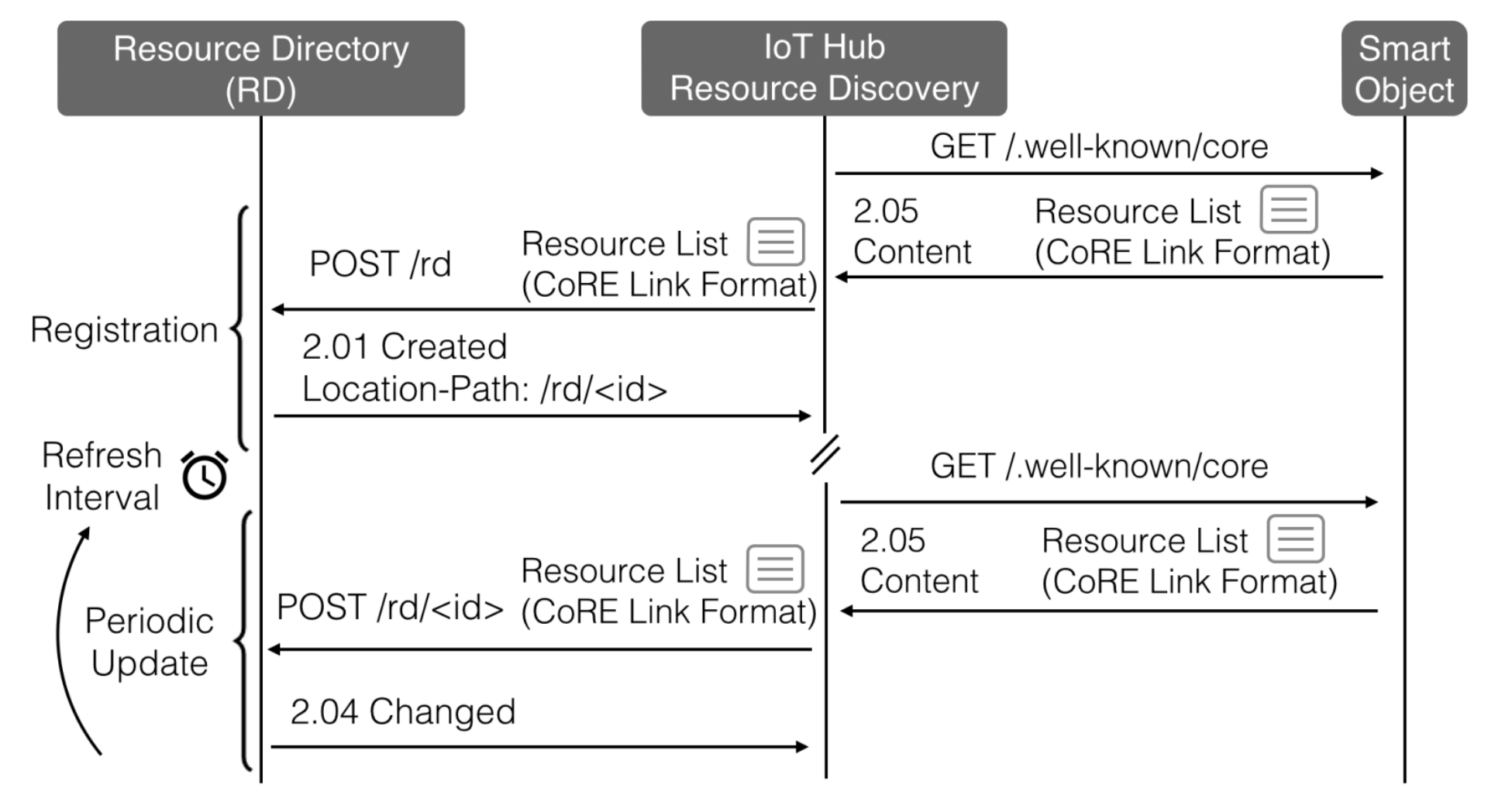
Is an specialized element that serves as a registry for all the resource in the overall IP network managed by the Iot Hub.

The RD provides:

○ a function set for the registration, update;

○ deletion of resources

○ a function set for the lookup of resources

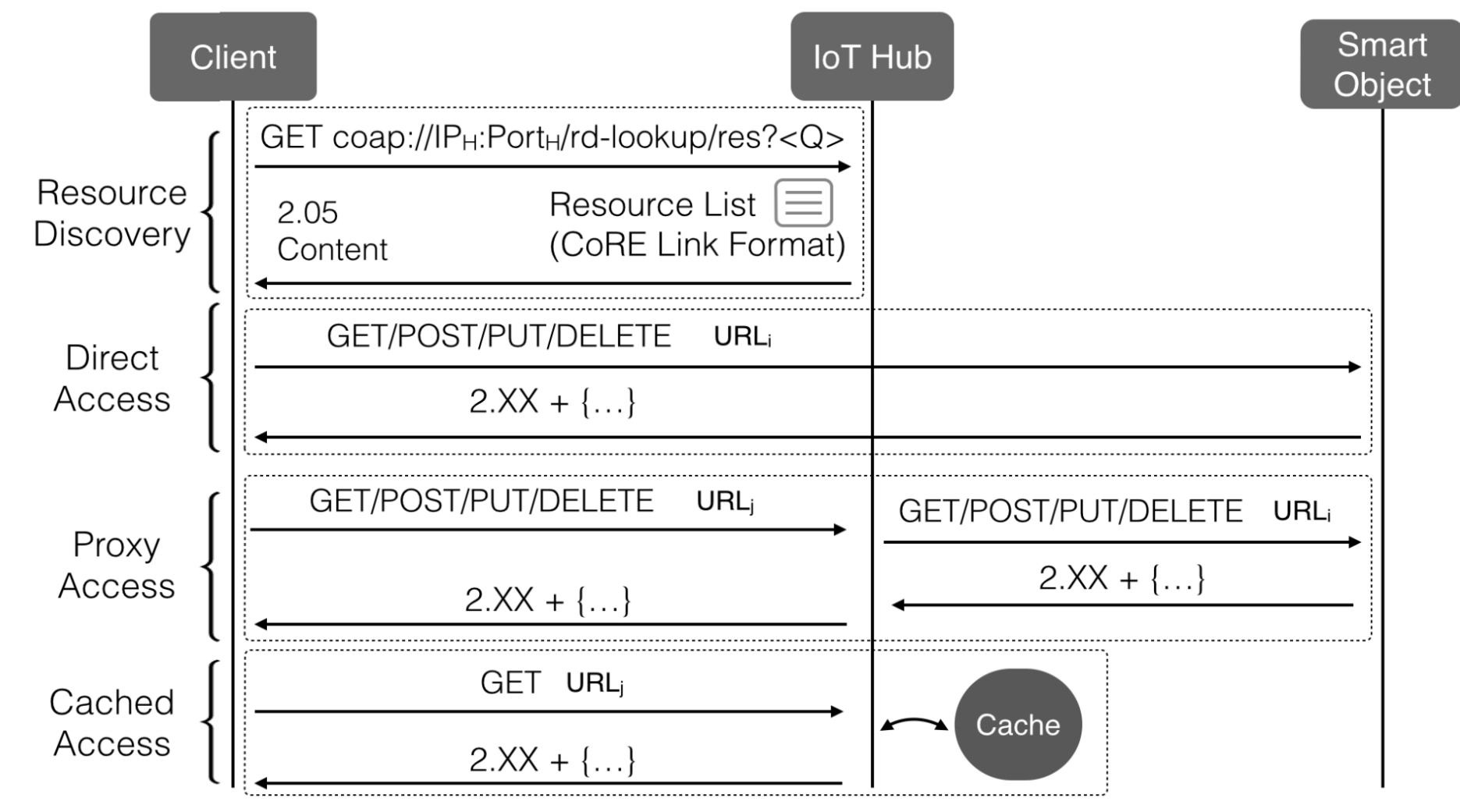


**Origin Server**

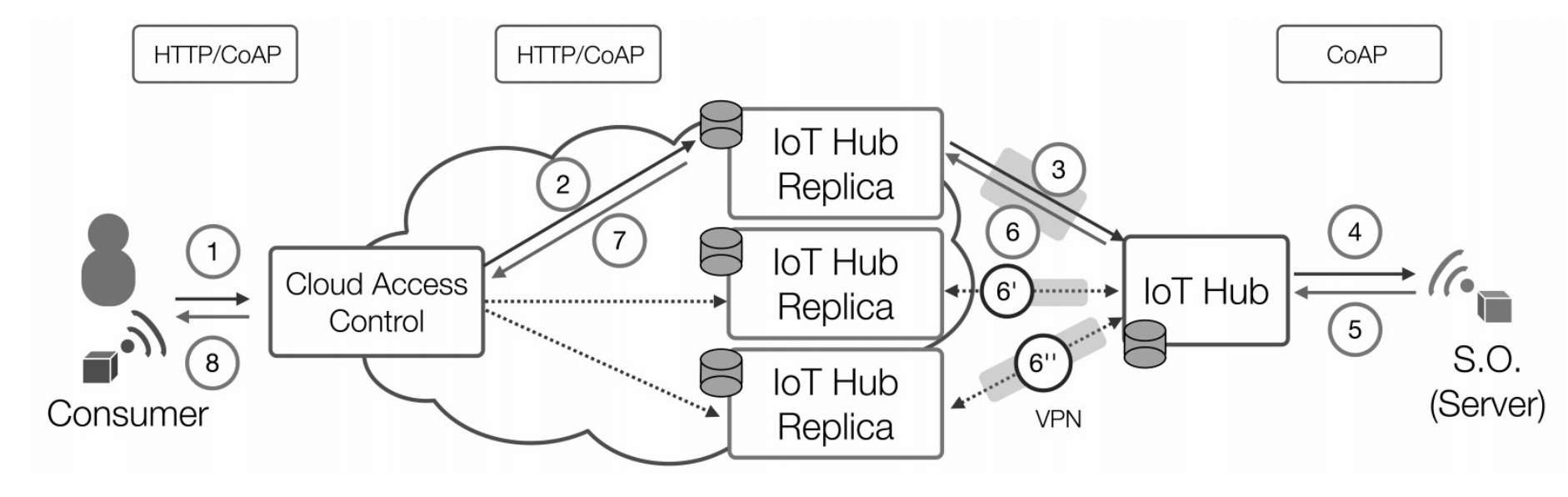
In some cases SOs have very limited capabilities and cannot host resources

The IoT hub offers a Origin server function

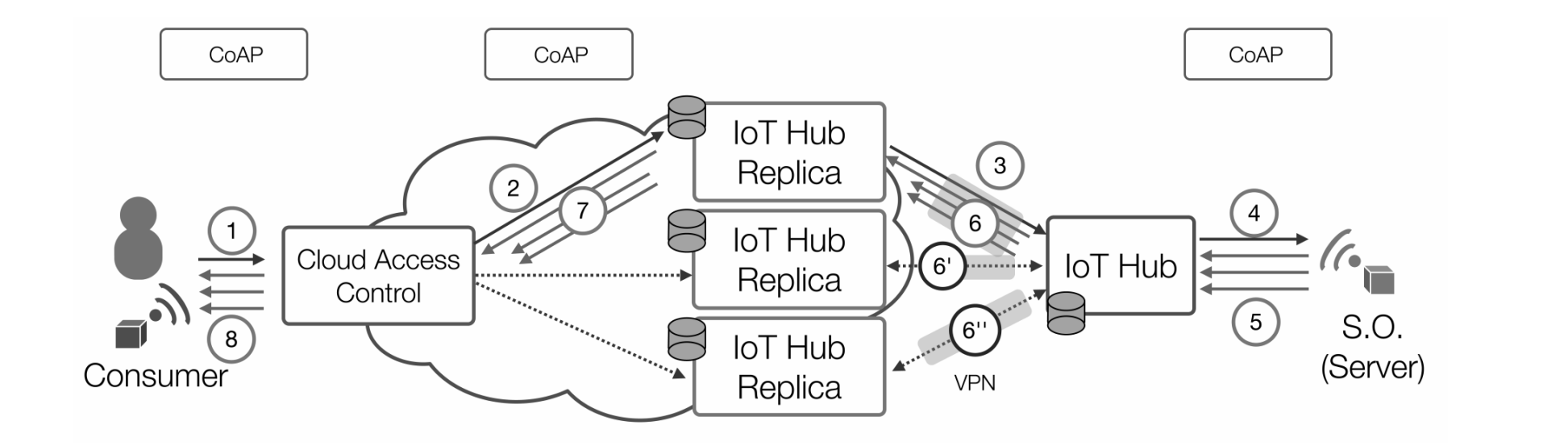
Clients can request to create and maintain a resource on their behalf  
**Iot Hub / Resource Access / Steps**



Using IoT Hub replica we are able to Polling Resources



Also using CoAP Observability and through IoT replica we can observe values



The syncing between the replicas is possible with a sync protocol