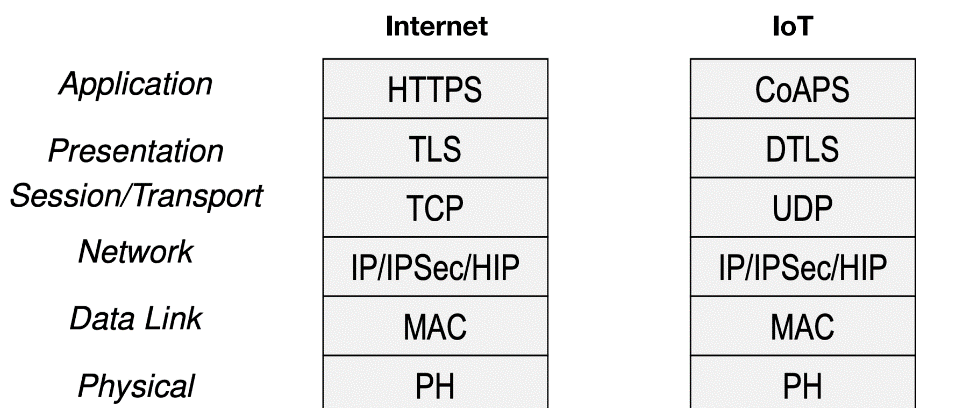
# Security

In the IoT field security can be difficult due to constrained devices.

Threats>

* Cloning of smart things
* Firmware replacement attack
* Extraction of security parameters from physically unprotected devices
* Eavesdropping attack ( No key )
* Main in the middle attacks (Spoofed key)
* Routing attack (routing altered or replayed)
* Privacy threat (your information can be sold to third parties)
* DDoS attack

**Countermeasures**

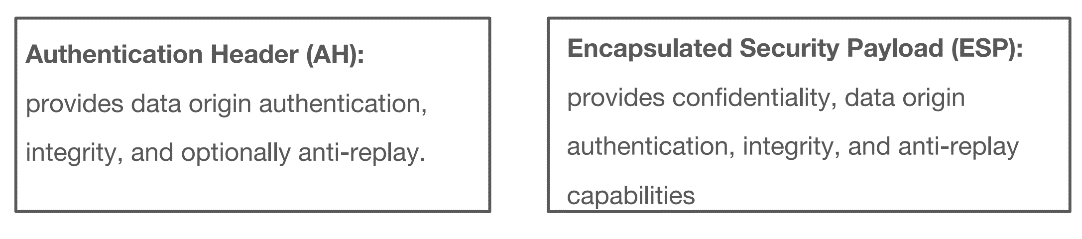
* Use of security protocols

Avoiding security service duplication

Interoperability

* Use of Internet Protocol Security

IPSec can provide

* Confidentiality
* Integrity
* Data-origin authentication
* Protection against replay attacks

This service are provided by two IPSec protocols, Authentication Header and Encapsulated Security Payload.

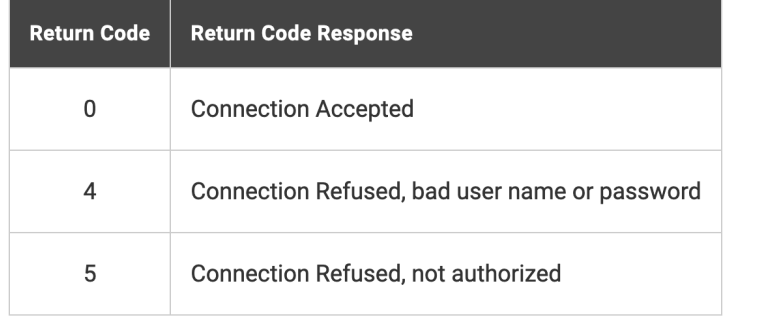
Obviously at the cost of Overhead

In transport layer instead od TLS is used **DTLS** 🡪 Datagram Transport Layer Security

Is used to provide security on top of UDP

It’s similar to TLS

**Security on MQTT**

A broker is not only responsible for persisting connection, as well as identifying and authorizing the transfer of data to MQTT clients.

Requires the client must report his id requesting a connection.

Once a broker receive a command from a client to connect it determines if the client is eligible to connect if the message receive contains a valid UID, username and password (optional)

In addition to authentication with username and password MQTT allows a device to auth with **a X.509** certificate.

(public key), is associated to TLS as its encryption method.