Subject:	LoRa gateway data flow details		
Products:	OCEAView, LoRa gateways, Cobalt X / L3 / ML3 data loggers		
Reference:	HOT-MO-20230324 EN		
Date:	March 2023	**Updated**:	-

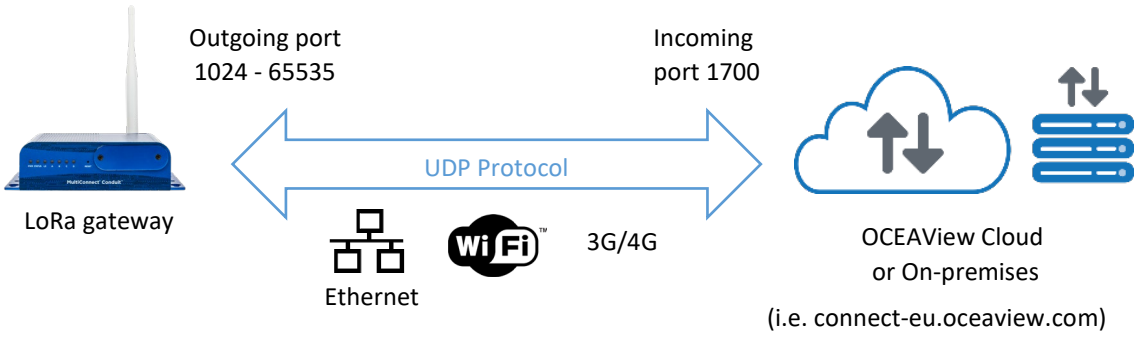
Introduction

The OCEAView solution comprises a set of interconnected software and hardware components that communicate with each other using specific technologies.

This document describes the flow of information exchanged via Dickson LoRa gateways from a network perspective, with details about the types of data flows involved and their characteristics.

OCEAView solution architecture

This diagram illustrates the flow of data from a Dickson LoRa gateway to the OCEAView platform



When using LoRa wireless connectivity, Dickson's Cobalt X, Cobalt L3, and Cobalt ML3 data loggers emit wireless data packets that are captured by all active and compatible LoRa gateways within wireless range. The gateways then transmit the data packets to the OCEAView Cloud platform or customer's private on-premises server.

Cobalt-series data loggers are not associated with a specific gateway. The data loggers also do not have any way to know whether a gateway has received emitted wireless data packets. From the data logger's perspective, packets are simply broadcast.

It is the gateway's task to forward data packets to the appropriate OCEAView platform. LoRa gateways are an intermediary tool that convert wireless packets from the data loggers into UDP (User Datagram Protocol) packets, and vice versa. Mechanisms on the OCEAView server are in charge of making sure that all information sent by the data loggers was received and recorded as expected.

All data transmitted by Cobalt X, L, and ML3 data loggers is encrypted and signed the using AES 128 advanced encryption standard in compliance with LoRaWAN protocol specifications.

Description of flows

Data flows (UDP): LoRa gateway ➔ OCEAView

Communication between the LoRa gateway and OCEAView server take place using the **UDP protocol**. The gateway **randomly chooses an outgoing port** (between 1024 and 65535) and seeks to connect to **port 1700** on the **OCEAView** server (for example: connect-eu.oceaview.com).

Communication is always initiated by the gateway. The server responds within seconds on the established communication channel.

The network infrastructure hosting the LoRa gateway must therefore authorize outgoing UDP communication from the gateway on any of the potential ports (1024 - 65535) it may use, towards port 1700 on the OCEAView server (i.e. connect-eu.oceaview.com).

To ensure proper operation, the following configurations must be verified:

- Firewall: must allow communication.
- Antivirus: must not cut off established connections prematurely.
- Load balancer: the outgoing data path must be identical to the return data path. If you use a load balancer, you must add a specific rule so that the path to and from the gateway is always the same for a given connection.

Status control flow of the active network interface (failover): ICMP

If a problem occurs with a network interface, the LoRa gateway can switch to a different interface. For example, if the gateway is operating on an Ethernet connection, it could switch to WiFi or cellular (4G). This failover mechanism is established using the PING (Packet Internet Groper) function to contact a server defined in the gateway's configuration. If the PING function fails repeatedly, the gateway switches to the backup network interface. The ICMP protocol, as well as access to the server indicated in the failover configuration (www.google.com by default), must be authorized.

Gateway clock synchronization (SNTP)

To keep its internal clock up to date, the gateway regularly connects to an NTP (Network Time Protocol) server. The SNTP protocol and NTP server must therefore also be authorized.