



**Arquitectura IoT Centrada en Pasarelas de Borde**  
Implementación de Protocolos basados en 6LowPAN para Smart Energy

**Juan Sebastian Giraldo Duque**

Facultad  
Departamento

Sede de la Universidad, Colombia (Nota: ciudad sede donde se gradúa [borrar esta nota])  
Año entrega

Nota: No utilizar el tipo de letra Ancizar en el documento puesto que este tipo de fuente restringe la copia de los archivos en el Repositorio Institucional. [Recuerde borrar esta nota]

# Arquitectura IoT Centrada en Pasarelas de Borde

Implementación de Protocolos basados en 6LowPAN para Smart Energy

**Juan Sebastian Giraldo Duque**

Tesis presentada como requisito parcial para optar por el título de:  
**Magíster (M, MSc) o Doctor (PhD) - Modalidad**

**Director(a):**

Prof. Dr. Director

Indicar si es Profesor Titular/Asociado - Departamento 2

Facultad

Universidad Nacional de Colombia

**Codirector(a):**

Prof. Dr. Co director

Indicar si es Profesor Titular/Asociado - Departamento

Facultad

Universidad Nacional de Colombia

**Línea de investigación:**

Línea

**Grupo de investigación:**

Grupo A (Sigla Grupo Investigación 01)

Grupo B (Sigla Grupo Investigación 02)

Universidad Nacional de Colombia

Facultad

Departamento

Año entrega

## Cita 01.

Autor  
*Fuente*

*Wenn du es nicht einfach erklären kannst, hast du es nicht genug verstanden - Si no eres capaz de explicar algo claramente, es que aún no lo has entendido lo suficiente.*

Albert Einstein

# Declaración

Me permito afirmar que he realizado ésta tesis de manera autónoma y con la única ayuda de los medios permitidos y no diferentes a los mencionados el presente texto. Todos los pasajes que se han tomado de manera textual o figurativa de textos publicados y no publicados, los he reconocido en el presente trabajo. Ninguna parte del presente trabajo se ha empleado en ningún otro tipo de tesis.

Sede de la Universidad., Fecha entrega

---

Juan Sebastian Giraldo Duque

# Agradecimientos

# Listado de símbolos y abreviaturas

# Resumen

## Arquitectura IoT Centrada en Pasarelas de Borde Implementación de Protocolos basados en 6LowPAN para Smart Energy

Texto del resumen.

**Palabras clave:** Use palabras clave que estén en Theasaurus

# Abstract

Nombre del trabajo o tesis en inglés

Abstract text.

**Keywords:** Use keywords available in Thesaurus

# Zusammenfassung

Nombre del trabajo o tesis en un tercer idioma

Zusammenfassung Texte.

Schlüsselwörter:

# Lista de figuras

5-1	Vista de despliegue ISO/IEC 30141 del gateway . . . . .	8
5-2	Arquitectura de contenedores del gateway OpenWRT . . . . .	14
6-1	Arquitectura completa del sistema de telemetría. . . . .	87

# Lista de tablas

<b>5-1</b>	Entidades funcionales ISO/IEC 30141 en el gateway . . . . .	8
<b>5-2</b>	Comparación Raspberry Pi 4 vs Router OpenWRT tradicional . . . . .	22
<b>5-3</b>	Comparación almacenamiento para gateway IoT . . . . .	26
<b>5-4</b>	Comparación de modos de operación HaLow . . . . .	34
<b>5-5</b>	Comparación de protocolos IoT . . . . .	45
<b>5-6</b>	Selección de protocolo por caso de uso . . . . .	50
<b>5-7</b>	Niveles de resiliencia en gateway con RTO (Recovery Time Objective). . . . .	53
<b>5-8</b>	Comparación de herramientas de gestión para gateway OpenWRT . . . . .	65
<b>5-9</b>	Comparación IA local vs cloud para gateway Smart Energy . . . . .	81
<b>5-10</b>	Casos de uso óptimos por modo de operación HaLow . . . . .	84
<b>5-11</b>	Comparación de soluciones HaLow comerciales (2025) . . . . .	85
<b>6-1</b>	Seguridad por capa . . . . .	94
<b>6-2</b>	Costos de implementación . . . . .	94

# Contenido

Agradecimientos	II
Listado de símbolos y abreviaturas	III
Resumen	IV
Abstract	V
Zusammenfassung	VI
Lista de figuras	VII
Lista de tablas	VIII
Contenido	IX
1 Planteamiento del Problema	1
2 Hipótesis	2
3 Objetivos	3
4 Marco teórico	4
5 Gateway de Telemetría para Smart Energy	5
5.1 Introducción . . . . .	5
5.1.1 Función del Gateway en la Arquitectura de Telemetría . . . . .	5
5.2 Conformidad con Estándares Internacionales . . . . .	6
5.2.1 IEEE 2030.5-2023 (Smart Energy Profile 2.0) . . . . .	6
5.2.2 ISO/IEC 30141:2024 (IoT Reference Architecture) . . . . .	7
5.3 Requisitos del Gateway . . . . .	9
5.3.1 Requisitos Funcionales . . . . .	9
5.3.2 Requisitos No Funcionales . . . . .	9
5.3.3 Requisitos de Seguridad . . . . .	10
5.4 Arquitectura Jerárquica de 3 Niveles IoT . . . . .	10
5.4.1 Nivel 1: Nodos IoT (End Devices) . . . . .	10
5.4.2 Nivel 2: Routers IoT . . . . .	11

## **Implementación de Protocolos basados en 6LowPAN para Smart Energy**

---

5.4.3	Nivel 3: Gateways IoT (Border Routers Edge) . . . . .	12
5.4.4	Flujo de Datos en Arquitectura de 3 Niveles . . . . .	13
5.5	Arquitectura de Software del Gateway . . . . .	13
5.5.1	Stack de Contenedores . . . . .	13
5.5.2	Stack de Comunicación . . . . .	14
5.5.3	Componentes de Software . . . . .	15
5.6	Flujo de Datos End-to-End . . . . .	18
5.6.1	Flujo Normal de Operación . . . . .	18
5.6.2	Flujo en Modo Edge (Sin Conectividad Cloud) . . . . .	19
5.6.3	Flujo de Comandos Downlink (Cloud → Dispositivo) . . . . .	19
5.6.4	Flujo de Actualización OTA de Contenedores . . . . .	19
5.7	Implementación del Gateway con OpenWRT . . . . .	19
5.7.1	Justificación de la Plataforma . . . . .	19
5.7.2	Hardware del Gateway . . . . .	20
5.8	Implementación en Raspberry Pi 4 con OpenWRT . . . . .	21
5.8.1	Hardware de la Implementación Real . . . . .	21
5.8.2	Sistema Operativo: OpenWRT 23.05 en Raspberry Pi 4 . . . . .	26
5.8.3	Configuración de Conectividad . . . . .	29
5.8.4	Configuración de Conectividad . . . . .	29
5.8.5	Instalación de Docker en OpenWRT . . . . .	36
5.8.6	Despliegue de OpenThread Border Router . . . . .	37
5.8.7	Integración OTBR ↔ ThingsBoard Edge . . . . .	39
5.9	Arquitectura de Datos: Kafka y PostgreSQL . . . . .	41
5.9.1	Integración de Apache Kafka . . . . .	41
5.9.2	PostgreSQL: Base de Datos Persistente . . . . .	44
5.10	Protocolos de Comunicación IoT . . . . .	45
5.10.1	Comparación de Protocolos . . . . .	45
5.10.2	MQTT (Message Queuing Telemetry Transport) . . . . .	45
5.10.3	CoAP (Constrained Application Protocol) . . . . .	46
5.10.4	HTTP/REST . . . . .	48
5.10.5	LwM2M (Lightweight M2M) . . . . .	48
5.10.6	Selección de Protocolo por Caso de Uso . . . . .	49
5.11	Resiliencia y Almacenamiento Persistente (SSD) . . . . .	49
5.11.1	Arquitectura de Almacenamiento del Gateway . . . . .	49
5.11.2	ThingsBoard Edge Queue: Resiliencia Offline . . . . .	51
5.11.3	Resiliencia Multinivel . . . . .	53
5.12	Gestión Remota del Gateway . . . . .	54
5.12.1	Feeds de OpenWRT . . . . .	54
5.12.2	OpenVPN: Acceso Remoto Seguro . . . . .	57
5.12.3	OpenWISP: Gestión Centralizada de Gateways . . . . .	60
5.12.4	Comparación de Herramientas de Gestión . . . . .	64
5.13	Gestión de Uplink Redundante (Ethernet + LTE) . . . . .	65
5.13.1	Política de Failover Automático . . . . .	65
5.13.2	Monitoreo Activo de Conectividad (mwan3) . . . . .	65

**Implementación de Protocolos basados en 6LowPAN para Smart Energy**

---

5.13.3	Optimización de Costos LTE . . . . .	66
5.14	Gestión y Monitoreo del Gateway . . . . .	68
5.14.1	Interfaz de Gestión (LuCI) . . . . .	68
5.14.2	Monitoreo de Contenedores . . . . .	68
5.14.3	Logs Centralizados . . . . .	69
5.14.4	Backups y Recuperación . . . . .	70
5.15	Pruebas y Validación . . . . .	71
5.15.1	Pruebas Funcionales . . . . .	71
5.15.2	Pruebas de Desempeño . . . . .	73
5.15.3	Pruebas de Seguridad . . . . .	74
5.15.4	Pruebas de Integración . . . . .	75
5.16	Integración de Inteligencia Artificial con MCP y LLM . . . . .	75
5.16.1	Arquitectura de IA en el Gateway . . . . .	75
5.16.2	Model Context Protocol (MCP) . . . . .	76
5.16.3	Despliegue de Ollama (LLM Local) . . . . .	76
5.16.4	MCP Server para ThingsBoard Edge . . . . .	77
5.16.5	Casos de Uso de IA en Gateway . . . . .	80
5.16.6	Ventajas de IA Local (Ollama + MCP) vs Cloud . . . . .	81
5.17	Conclusiones del Capítulo . . . . .	81
5.17.1	Casos de Uso Óptimos por Modo HaLow . . . . .	84
5.17.2	Ventajas de Morse Micro sobre Alternativas HaLow . . . . .	85
5.17.3	Limitaciones y Trabajo Futuro . . . . .	85
<b>6</b>	<b>Arquitectura de Telemetría para Smart Energy</b>	<b>87</b>
6.1	Introducción . . . . .	87
6.2	Visión General de la Arquitectura . . . . .	87
6.2.1	Componentes Principales . . . . .	87
6.3	Capa de Dispositivos: Medidores Inteligentes . . . . .	88
6.3.1	Características de los Medidores . . . . .	88
6.3.2	Interfaz de Lectura . . . . .	88
6.4	Capa de Campo: Nodos y DCUs . . . . .	88
6.4.1	Nodos Adaptadores RS485 + ESP32C6 + Thread . . . . .	88
6.4.2	DCU (Data Concentrator Unit) . . . . .	89
6.5	Topología de Red Thread . . . . .	90
6.5.1	Mesh Networking . . . . .	90
6.5.2	Ventajas de Thread . . . . .	90
6.5.3	Configuración de Red . . . . .	90
6.6	Backhaul: 802.11ah (HaLow) . . . . .	91
6.6.1	Justificación de HaLow . . . . .	91
6.6.2	Configuración HaLow . . . . .	91
6.6.3	Topología HaLow . . . . .	91
6.7	Gateway y Uplink a Cloud . . . . .	91
6.7.1	Resumen de Funciones . . . . .	92
6.8	Capa de Aplicación: ThingsBoard . . . . .	92

## **Implementación de Protocolos basados en 6LowPAN para Smart Energy**

---

6.8.1	Funcionalidades . . . . .	92
6.8.2	Modelo de Datos en ThingsBoard . . . . .	92
6.9	Caso de Estudio: Despliegue en Smart Energy . . . . .	93
6.9.1	Escenario . . . . .	93
6.9.2	Dimensionamiento . . . . .	93
6.9.3	Resiliencia y Redundancia . . . . .	93
6.9.4	Seguridad End-to-End . . . . .	94
6.10	Ánalisis de Costos . . . . .	94
6.10.1	Costos de Hardware (estimado) . . . . .	94
6.10.2	Comparación con Alternativas . . . . .	94
6.11	Métricas de Desempeño . . . . .	94
6.11.1	Latencia E2E . . . . .	94
6.11.2	Disponibilidad . . . . .	95
6.11.3	Pérdida de Datos . . . . .	95
6.12	Escalabilidad . . . . .	95
6.12.1	Crecimiento Horizontal . . . . .	95
6.12.2	Límites Teóricos . . . . .	95
6.13	Trabajos Futuros y Mejoras . . . . .	95
6.13.1	Mejoras Propuestas . . . . .	95
6.13.2	Integración con Blockchain . . . . .	96
6.14	Conclusiones del Capítulo . . . . .	96
<b>7</b>	<b>Discusión de resultados</b>	<b>97</b>
<b>8</b>	<b>Conclusiones</b>	<b>98</b>
<b>9</b>	<b>Recomendaciones</b>	<b>99</b>
<b>A</b>	<b>Apéndice 1</b>	<b>101</b>
<b>B</b>	<b>Instalación y Configuración del Gateway OpenWRT</b>	<b>102</b>
B.1	Sistema Operativo: OpenWRT 23.05 . . . . .	102
B.1.1	Especificaciones de la Versión . . . . .	102
B.1.2	Procedimiento de Instalación . . . . .	102
B.1.3	Instalación de Paquetes Esenciales . . . . .	104
B.2	Configuración de Almacenamiento NVMe . . . . .	105
B.2.1	Detección y Particionamiento del SSD . . . . .	105
B.2.2	Montaje Automático en /mnt/ssd . . . . .	105
B.2.3	Estructura de Directorios para Servicios . . . . .	106
B.2.4	Configuración de Docker para usar SSD . . . . .	106
B.3	Configuración de Periféricos de Conectividad . . . . .	107
B.3.1	Thread Border Router con nRF52840 Dongle . . . . .	107
B.3.2	HaLow 802.11ah via SPI (Morse Micro MM6108) . . . . .	109
B.3.3	LTE Modem Quectel BG95-M3 . . . . .	111
B.4	Instalación de Docker y Docker Compose . . . . .	113

**Implementación de Protocolos basados en 6LowPAN para Smart Energy**

---

B.4.1	Instalación de Paquetes Docker . . . . .	113
B.4.2	Configuración de Docker Daemon . . . . .	114
B.5	Verificación de Instalación Completa . . . . .	115
B.5.1	Checklist de Verificación . . . . .	115
B.5.2	Logs de Sistema para Debug . . . . .	116
B.6	Troubleshooting Común . . . . .	116
B.6.1	Problemas con NVMe SSD . . . . .	116
B.6.2	Problemas con Thread nRF52840 . . . . .	117
B.6.3	Problemas con HaLow SPI . . . . .	117
B.6.4	Problemas con LTE Quectel . . . . .	117
B.7	Resumen de Configuración . . . . .	118
<b>C</b>	<b>Archivos Docker Compose del Gateway</b>	<b>119</b>
C.1	Estructura de Directorios Docker . . . . .	119
C.2	OpenThread Border Router (OTBR) . . . . .	120
C.2.1	Función del OTBR . . . . .	120
C.2.2	Docker Compose: OTBR . . . . .	120
C.2.3	Comandos de Gestión OTBR . . . . .	121
C.3	ThingsBoard Edge + PostgreSQL . . . . .	121
C.3.1	Función de ThingsBoard Edge . . . . .	121
C.3.2	Docker Compose: ThingsBoard Edge . . . . .	122
C.3.3	Archivo .env para Variables de Entorno . . . . .	123
C.3.4	Comandos de Gestión ThingsBoard Edge . . . . .	123
C.4	IEEE 2030.5 Server (SEP 2.0) . . . . .	124
C.4.1	Función del IEEE 2030.5 Server . . . . .	124
C.4.2	Docker Compose: IEEE 2030.5 Server . . . . .	124
C.4.3	Dockerfile para IEEE 2030.5 Server . . . . .	125
C.4.4	requirements.txt . . . . .	126
C.5	Apache Kafka + Zookeeper . . . . .	126
C.5.1	Función de Kafka . . . . .	126
C.5.2	Docker Compose: Kafka . . . . .	126
C.5.3	Comandos de Gestión Kafka . . . . .	128
C.6	Bridge Thread-ThingsBoard . . . . .	129
C.6.1	Función del Bridge . . . . .	129
C.6.2	Docker Compose: Bridge . . . . .	129
C.6.3	Dockerfile para Bridge . . . . .	130
C.7	Orquestación Completa con docker-compose . . . . .	130
C.7.1	Comandos de Gestión Global . . . . .	130
C.8	Resumen . . . . .	131
<b>D</b>	<b>Anexo C: Scripts y Código de Integración</b>	<b>132</b>
D.1	Servidor IEEE 2030.5 (SEP 2.0) . . . . .	132
D.1.1	Aplicación Flask Principal . . . . .	132
D.1.2	Dockerfile . . . . .	136

<b>Implementación de Protocolos basados en 6LowPAN para Smart Energy</b>	
D.1.3 requirements.txt . . . . .	137
D.2 Bridge Thread ↔ ThingsBoard Edge . . . . .	137
D.2.1 Script Bridge Principal . . . . .	137
D.2.2 Dockerfile del Bridge . . . . .	141
D.2.3 requirements_bridge.txt . . . . .	142
D.3 Integración con Apache Kafka . . . . .	142
D.3.1 Productor Kafka . . . . .	142
D.3.2 Consumidor Kafka . . . . .	144
D.3.3 requirements_kafka.txt . . . . .	146
D.4 Scripts de Gestión . . . . .	146
D.4.1 Comandos de Verificación . . . . .	146
D.4.2 Backup de Configuraciones . . . . .	147
<b>E Anexo D: Especificaciones IEEE 2030.5 y Configuraciones</b>	148
E.1 Ejemplos XML IEEE 2030.5 . . . . .	148
E.1.1 Device Capability (DCAP) . . . . .	148
E.1.2 Time Synchronization (TM) . . . . .	148
E.1.3 Mirror Usage Point (MUP) . . . . .	149
E.1.4 End Device List . . . . .	151
E.2 Configuraciones UCI para HaLow 802.11ah . . . . .	152
E.2.1 Modo Access Point (AP) . . . . .	152
E.2.2 Modo Station (STA) . . . . .	153
E.2.3 Modo Mesh 802.11s . . . . .	154
E.2.4 Modo EasyMesh (IEEE 1905.1) . . . . .	156
E.3 Optimización TimescaleDB . . . . .	157
E.3.1 Configuración PostgreSQL + TimescaleDB . . . . .	157
E.3.2 Schema y Hypertables . . . . .	158
E.3.3 Queries de Ejemplo . . . . .	159
E.3.4 Mantenimiento . . . . .	160
E.4 Generación de Certificados X.509 para mTLS . . . . .	161
E.4.1 Autoridad Certificadora (CA) . . . . .	161
E.4.2 Certificado Servidor IEEE 2030.5 . . . . .	161
E.4.3 Certificado Cliente SEP 2.0 . . . . .	161
E.4.4 Prueba mTLS . . . . .	162
<b>F Anexo E: Implementación Nodo IoT de Referencia</b>	163
F.1 Arquitectura del Nodo . . . . .	163
F.1.1 Hardware . . . . .	163
F.1.2 Stack de Software . . . . .	163
F.2 Código Principal . . . . .	164
F.2.1 main.c . . . . .	164
F.3 Cliente LwM2M . . . . .	166
F.3.1 lwm2m_client.c (fragmento principal) . . . . .	166
F.4 Objetos IPSO . . . . .	171

**Implementación de Protocolos basados en 6LowPAN para Smart Energy**

---

F.4.1 temp_object.c . . . . .	171
F.4.2 humidity_object.c . . . . .	174
F.5 Objetos LwM2M Core . . . . .	176
F.5.1 device_object.c (fragmento) . . . . .	176
F.6 Conectividad Thread . . . . .	178
F.6.1 thread_prov.c (fragmento) . . . . .	178
F.7 CMakeLists.txt . . . . .	180
F.7.1 Configuración de Build . . . . .	180
F.8 sdkconfig.defaults . . . . .	181
F.8.1 Configuración por Defecto . . . . .	181
F.9 Uso del Nodo . . . . .	182
F.9.1 Compilación y Flash . . . . .	182
F.9.2 Comisionamiento Thread . . . . .	182
F.9.3 Verificación LwM2M . . . . .	182
<b>Referencias Bibliográficas</b>	<b>184</b>

# 1 Planteamiento del Problema

## 2 Hipótesis

### 3 Objetivos

## 4 Marco teórico

# 5 Gateway de Telemetría para Smart Energy

## 5.1 Introducción

El gateway constituye el componente central de la arquitectura de telemetría propuesta. Este dispositivo actúa como puente entre las redes de campo (802.15.4/Thread) y las redes de área amplia (802.11ah/HaLow), consolidando datos de múltiples medidores inteligentes y transmitiéndolos de manera segura hacia la plataforma IoT en la nube.

### 5.1.1 Función del Gateway en la Arquitectura de Telemetría

En el contexto de infraestructuras de medición inteligente para Smart Energy, el gateway cumple las siguientes funciones críticas:

- **Agregación de datos:** Recopila información de múltiples DCUs (Data Concentrator Units) que gestionan clústeres de medidores.
- **Protocol translation:** Realiza la conversión entre protocolos de red de área local (Thread/802.15.4) y protocolos de aplicación cloud (MQTT/TLS).
- **Seguridad:** Implementa cifrado end-to-end mediante TLS/mTLS, autenticación mutua y gestión de certificados.
- **Resiliencia:** Proporciona buffering local, manejo de desconexiones y reinicio automático ante fallos de conectividad.
- **Edge computing:** Permite preprocesamiento local de datos, filtrado y compresión antes de la transmisión.

## 5.2 Conformidad con Estándares Internacionales

### 5.2.1 IEEE 2030.5-2023 (Smart Energy Profile 2.0)

El gateway implementa funcionalidades alineadas con IEEE 2030.5 (SEP 2.0), el estándar para aplicaciones de Smart Energy sobre TCP/IP. Este estándar define una arquitectura RESTful para gestión de energía del usuario final, incluyendo respuesta a la demanda, control de carga, precios dinámicos y recursos energéticos distribuidos (DER).

#### Function Sets Implementados

El gateway soporta los siguientes *Function Sets* de IEEE 2030.5:

1. **Device Capability (DCAP)**: Descubrimiento de capacidades del gateway y endpoints.
  - Recurso: /dcap
  - Expone: MeteringMirror, Time, Messaging, EndDevice List.
2. **Time (TM)**: Sincronización horaria NTP/PTP para timestamps precisos.
  - Recurso: /tm
  - Precisión: <100 ms (suficiente para facturación).
3. **Metering Mirror (MM)**: Reflejo de datos de medición para lectura por utilidades.
  - Recurso: /mup/{deviceID}/MirrorUsagePoint
  - Datos: Energía activa (Wh), reactiva (VArh), demanda (W).
  - Granularidad: 15 min (alineado con IEC 62056).
4. **Messaging (MSG)**: Notificaciones y alertas bidireccionales.
  - Texto simple para eventos críticos (cortes, sobrecarga).
5. **End Device (ED)**: Registro y gestión de dispositivos.
  - Recurso: /eudev
  - Identificación: LFDI (Long Form Device Identifier) basado en certificado X.509.

#### Arquitectura RESTful

El gateway expone una API REST HTTP/TLS compatible con IEEE 2030.5. El siguiente ejemplo ilustra una consulta típica de telemetría:

```
# Ejemplo: Consultar telemetría de medidor
GET https://gateway:8883/mup/0123456789ABCDEF/MirrorUsagePoint
Authorization: Bearer <JWT-TOKEN>

# Respuesta (XML IEEE 2030.5)
```

```

<MirrorUsagePoint>
  <mRID>0123456789ABCDEF</mRID>
  <MirrorMeterReading>
    <Reading>
      <value>1234567</value>  <!-- Wh acumulado -->
      <timePeriod>
        <duration>900</duration>  <!-- 15 min -->
        <start>1730000000</start>
      </timePeriod>
    </Reading>
  </MirrorMeterReading>
</MirrorUsagePoint>

```

*Nota:* Los ejemplos completos de respuestas XML IEEE 2030.5 para todos los Function Sets (DCAP, Time, Mirror Usage Point, End Device List, Messaging) se presentan en el Anexo D.

## Seguridad IEEE 2030.5

- **TLS 1.2/1.3 obligatorio:** Todas las comunicaciones cifradas.
- **Certificados X.509 ECC:** Autenticación mutua con curva P-256.
- **LFDI derivado de certificado:** SHA-256(SubjectPublicKeyInfo)[0:20].
- **Role-Based Access Control (RBAC):** Permisos según rol del cliente (utility, usuario, DER).

### 5.2.2 ISO/IEC 30141:2024 (IoT Reference Architecture)

ISO/IEC 30141 define una arquitectura de referencia para sistemas IoT con cuatro vistas: funcional, información, despliegue y operacional. El gateway implementa múltiples entidades funcionales de este modelo:

#### Vista Funcional del Gateway

#### Vista de Información

El gateway maneja los siguientes modelos de información:

- **Device Model:** Metadatos de medidores (ID, ubicación, tipo, características).
- **Observation Model:** Telemetría (timestamps, valores, calidad, unidades).
- **Command Model:** Instrucciones a dispositivos (cambio de intervalo, desconexión).
- **Event Model:** Notificaciones de eventos (alarmas, cortes, reconexiones).

Estos modelos se mapean a:

Entidad Funcional	Función	Implementación
Sensing	Recepción de datos de sensores (medidores) via Thread/HaLow	OTBR + bridge Python
Actuation	Envío de comandos a dispositivos (ej. desconexión)	MQTT RPC + CoAP
Processing	Procesamiento local (agregación, normalización)	ThingsBoard Edge Rule Engine
Storage	Almacenamiento persistente de datos y configuración	PostgreSQL + ext4
Communication	Gestión de protocolos (Thread, HaLow, LTE, Ethernet)	OpenWRT netifd + Docker
Security	Autenticación, cifrado, control de acceso	TLS/mTLS, WPA3- SAE, nftables
Management	Configuración, monitoreo, actualización OTA	LuCI + Watchtower + mwlan3
Application Support	APIs para aplicaciones (REST, MQTT)	TB Edge API + IEEE 2030.5 endpoints

Tabla 5-1: Entidades funcionales ISO/IEC 30141 en el gateway

- IEEE 2030.5: MirrorUsagePoint, EndDevice, Reading.
- ThingsBoard: Device, Telemetry, Attributes, RPC.
- OBIS/DLMS: Códigos IEC 62056 (ej. 1-0:1.8.0 = energía activa total).

## Vista de Despliegue

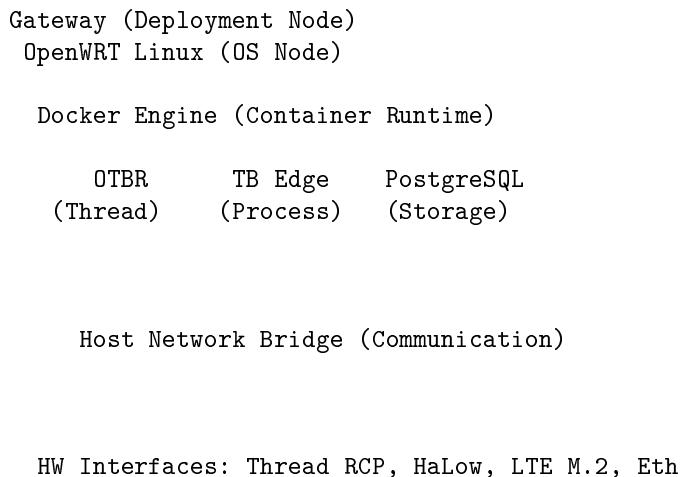


Figura 5-1: Vista de despliegue ISO/IEC 30141 del gateway

## Vista Operacional

Actividades operacionales según ISO/IEC 30141:

- **Provisioning:** Configuración inicial vía LuCI o CLI (UCI).
- **Monitoring:** Healthchecks Docker, vnstat (tráfico), mwan3 (WAN), logs syslog.
- **Maintenance:** Actualizaciones OTA con Watchtower, backups automatizados.
- **Fault Management:** Failover WAN automático, restart de contenedores no-healthy.

## 5.3 Requisitos del Gateway

### 5.3.1 Requisitos Funcionales

1. **RF-GW-001:** El gateway debe recibir datos de al menos 10 DCUs simultáneamente mediante 802.11ah (HaLow).
2. **RF-GW-002:** Debe normalizar y transformar datos OBIS de DLMS/COSEM a formato JSON/CBOR.
3. **RF-GW-003:** Debe publicar telemetría a broker MQTT con QoS 1 o 2 garantizando entrega.
4. **RF-GW-004:** Debe soportar topics MQTT estructurados: `telemetry/{region}/{dcu}/{meter}`.
5. **RF-GW-005:** Debe mantener buffer persistente local (ext4) con capacidad mínima de 7 días.
6. **RF-GW-006:** Debe soportar uplink redundante: Ethernet WAN (primario) y LTE M.2 (backup automático).
7. **RF-GW-007:** Debe operar como Access Point HaLow (902-928 MHz) con alcance mínimo de 1 km.
8. **RF-GW-008 (IEEE 2030.5):** Debe exponer API REST compatible con IEEE 2030.5 Function Sets: DCAP, TM, MM, MSG, ED.
9. **RF-GW-009 (IEEE 2030.5):** Debe implementar MirrorUsagePoint para lectura de telemetría con granularidad de 15 minutos.
10. **RF-GW-010 (ISO/IEC 30141):** Debe implementar entidades funcionales: Sensing, Processing, Storage, Communication, Security, Management.

### 5.3.2 Requisitos No Funcionales

1. **RNF-GW-001:** Latencia E2E (DCU→Gateway→Cloud) menor a 5 segundos para lecturas instantáneas.
2. **RNF-GW-002:** Disponibilidad mayor al 99.5 % con failover automático Ethernet LTE en <30 seg.
3. **RNF-GW-003:** Consumo energético en modo activo menor a 15W (con LTE en idle).
4. **RNF-GW-004:** Operación en rango de temperatura -10°C a +50°C (Morse Micro: -40°C a +85°C).
5. **RNF-GW-005:** Throughput HaLow: mínimo 20 Mbps agregado (suficiente para 10 DCUs @ 2 Mbps c/u).
6. **RNF-GW-006 (IEEE 2030.5):** Precisión de sincronización horaria <100 ms para timestamping de lecturas.
7. **RNF-GW-007 (IEEE 2030.5):** Soporte de al menos 250 EndDevices simultáneos (vía DCUs).

### 5.3.3 Requisitos de Seguridad

1. **RS-GW-001:** Autenticación mutua TLS 1.2/1.3 con broker MQTT y ThingsBoard Cloud.
2. **RS-GW-002:** Certificados X.509 con renovación automática antes de expiración.
3. **RS-GW-003:** Secure Boot habilitado para prevenir firmware no autorizado.
4. **RS-GW-004:** Cifrado de credenciales y llaves en memoria no volátil (UCI encrypt).
5. **RS-GW-005:** OTA (Over-The-Air) segura con validación de firma digital de imágenes Docker.
6. **RS-GW-006 (IEEE 2030.5):** Certificados ECC P-256 para autenticación de EndDevices.
7. **RS-GW-007 (IEEE 2030.5):** LFDI (Long Form Device Identifier) derivado de certificado X.509.
8. **RS-GW-008 (IEEE 2030.5):** RBAC (Role-Based Access Control) para APIs REST.
9. **RS-GW-009:** WPA3-SAE con PMF obligatorio en interfaz HaLow.

## 5.4 Arquitectura Jerárquica de 3 Niveles IoT

La arquitectura propuesta sigue un modelo jerárquico de tres niveles que optimiza la distribución de funciones, consumo energético y capacidad de procesamiento en redes IoT de gran escala. Esta arquitectura, alineada con las implementaciones de referencia de Morse Micro para Wi-Fi HaLow *Morse Micro* [2025], permite desplegar redes IoT con miles de dispositivos manteniendo eficiencia operativa y escalabilidad.

### 5.4.1 Nivel 1: Nodos IoT (End Devices)

El primer nivel está compuesto por dispositivos sensores y actuadores de bajo consumo energético, optimizados para operación con baterías durante años. Estos nodos implementan las funciones mínimas necesarias para:

- **Adquisición de datos:** Sensores de temperatura, humedad, consumo eléctrico, calidad del aire, etc.
- **Actuación:** Control de válvulas, relés, displays, alarmas.
- **Conectividad:** Thread (802.15.4) o HaLow 802.11ah en modo cliente (STA).
- **Protocolos de aplicación:** LwM2M (Lightweight M2M) sobre CoAP, MQTT-SN, IEEE 2030.5 Client.

### Características de Nodos IoT

- **Hardware:** Microcontroladores de bajo consumo (Arm Cortex-M4/M33): ESP32-C6, nRF52840, STM32U5, etc.
- **RAM/Flash:** 256 KB - 1 MB RAM, 1-4 MB Flash.
- **Modos de ahorro:** Sleep profundo, wake-on-radio, duty cycling <1 %.

- **Autonomía:** 5-10 años con batería AA (2600 mAh) en aplicaciones de telemetría con reportes cada 15 min.
- **Stack de software:** RTOS ligero (FreeRTOS, Zephyr), stack Thread/Matter o driver HaLow STA.

**Ejemplo de implementación:** Nodo de telemetría de temperatura y humedad basado en ESP32 con ESP-IDF, cliente LwM2M (AVSystems Anjay), conectividad Thread vía nRF52840 RCP. La implementación de referencia se detalla en el Anexo E.

#### 5.4.2 Nivel 2: Routers IoT

El segundo nivel está formado por routers IoT que extienden el alcance de las redes HaLow o Thread, actuando como repetidores inteligentes. Estos dispositivos tienen mayor capacidad que los nodos, pero menor que los gateways, optimizados para:

- **Routing multi-hop:** Mesh 802.11s, EasyMesh (IEEE 1905.1), Thread Router.
- **Conectividad:** HaLow en modo AP + STA simultáneo (repetidor), Thread Router.
- **Funciones limitadas:** Forwarding de paquetes, discovery de vecinos, sin procesamiento de aplicación.

#### Características de Routers IoT

- **Hardware:** SoC HaLow Morse Micro MM8108 + MPU Linux ligero (MediaTek MT7981B, MT7688).
- **RAM/Flash:** 128-256 MB RAM, 16-32 MB Flash.
- **Sistema Operativo:** OpenWRT mínimo, sin Docker ni bases de datos.
- **Alimentación:** PoE (802.3af/at), DC 12V, ocasionalmente baterías de respaldo.
- **Ejemplos comerciales:** GLi.net GL-MT3000 con módulo MM8108 (GLi.net GL-MT3000 + MM8108-EKH19 EVK) *Morse Micro [2025]*.

#### Diferencias con Gateways

Los routers IoT **no** implementan:

- Border Router completo (sin traducción Thread ↔ IP externa).
- Procesamiento edge (sin Docker, sin bases de datos).
- Conectividad WAN celular (LTE/5G).
- Interfaces IEEE 2030.5 Server o ThingsBoard Edge.

Su función es puramente de **extensión de cobertura** y **densificación de la red**, permitiendo que nodos IoT alejados del gateway alcancen conectividad mediante saltos intermedios.

### 5.4.3 Nivel 3: Gateways IoT (Border Routers Edge)

El tercer nivel lo constituyen los gateways IoT, dispositivos con capacidades de cómputo significativas que actúan como puntos de agregación, procesamiento edge y puente entre redes IoT locales (Thread, HaLow) y redes WAN (Internet, LTE). Este es el nivel que se desarrolla en profundidad en el presente capítulo.

#### Características de Gateways IoT

- **Hardware:** Plataformas ARM Cortex-A con múltiples núcleos: Raspberry Pi 4 (BCM2711), Banana Pi, Orange Pi, NanoPi R5S.
- **RAM/Flash:** 4-8 GB RAM, 64-256 GB NVMe SSD.
- **Conectividad múltiple:** HaLow AP/Mesh, Thread Border Router, LTE/5G, Ethernet Gigabit, Wi-Fi 6.
- **Sistema Operativo:** OpenWRT 23.05 con Docker, UCI, kernel completo con módulos NVMe/USB/SPI.
- **Funciones avanzadas:**
  - **Border Routing:** Thread ↔ IPv6, HaLow ↔ Ethernet/LTE.
  - **Edge Computing:** ThingsBoard Edge, PostgreSQL, TimescaleDB, reglas locales, dashboards.
  - **Protocolos Smart Energy:** IEEE 2030.5 Server (SEP 2.0), OpenADR, OCPP.
  - **Message Brokers:** Apache Kafka, Mosquitto MQTT, RabbitMQ.
  - **Orquestación:** Docker Compose, actualizaciones OTA de contenedores.
  - **Almacenamiento local:** PostgreSQL + TimescaleDB para series temporales, buffer en caso de desconexión cloud.
- **Alimentación:** PoE+ (802.3at/bt, 25-60W), DC 12V/5A.

#### Justificación del Modelo de 3 Niveles

La arquitectura jerárquica ofrece ventajas significativas frente a topologías planas:

1. **Escalabilidad:** Un gateway puede gestionar 100-200 nodos directamente. Con routers intermedios, la red puede escalar a 1000+ nodos mediante saltos múltiples.
2. **Eficiencia energética:** Los nodos no necesitan potencia de transmisión alta para alcanzar el gateway; pueden comunicarse con routers cercanos en saltos cortos (menor consumo).
3. **Cobertura extendida:** HaLow ofrece >1 km en línea de vista. Con routers mesh, la cobertura puede alcanzar 3-5 km en entornos urbanos.
4. **Resiliencia:** Si un router falla, el protocolo mesh reconfigura rutas automáticamente. El gateway permanece como punto de agregación estable.
5. **Distribución de carga:** El gateway concentra procesamiento pesado (bases de datos, analytics, cloud sync); los routers solo routing; los nodos solo sensing.
6. **Costo optimizado:** Desplegar pocos gateways costosos (RPi4 + NVMe + LTE) y múltiples routers económicos (MM8108 + MediaTek \$30 USD) es más rentable que múltiples gateways.

#### 5.4.4 Fluo de Datos en Arquitectura de 3 Niveles

El flujo típico de telemetría en la arquitectura propuesta sigue la siguiente secuencia:

1. **Nodo IoT** (Nivel 1): El sensor adquiere temperatura ( $23.5^{\circ}\text{C}$ ) y la empaqueta en mensaje LwM2M/CoAP o IEEE 2030.5 XML.
2. **Transmisión Thread/HaLow**: El nodo transmite el mensaje al router más cercano (RSSI óptimo) mediante protocolo Thread o HaLow STA.
3. **Router IoT** (Nivel 2): Recibe el mensaje, verifica integridad, y lo reenvía al gateway mediante routing mesh (posiblemente con saltos intermedios adicionales).
4. **Gateway IoT** (Nivel 3): Recibe el mensaje en interfaz Thread (OTBR) o HaLow (wlan-ah0).
5. **Procesamiento Edge**: El gateway ejecuta:
  - Conversión de protocolo (CoAP → MQTT, IEEE 2030.5 → JSON).
  - Validación de datos (rango esperado, detección de anomalías).
  - Almacenamiento en PostgreSQL/TimescaleDB.
  - Publicación en topic Kafka para analytics locales.
  - Envío a ThingsBoard Edge para visualización en dashboard local.
6. **Sincronización Cloud**: El gateway sincroniza datos con ThingsBoard Cloud vía LTE/Ethernet (cuando hay conectividad). Si no hay WAN, los datos quedan en buffer local hasta recuperar conectividad.

En sentido inverso (comandos downlink desde cloud), el flujo es:

1. **ThingsBoard Cloud** envía comando RPC al gateway (ej: apagar actuador).
2. **Gateway** recibe comando, valida permisos (RBAC), y traduce a protocolo del nodo (LwM2M Write, IEEE 2030.5 DER Control).
3. **Router(s)** reenvía(n) el comando al nodo destino mediante mesh.
4. **Nodo** ejecuta acción (apagar relé) y responde con ACK.
5. **Gateway** confirma ejecución a cloud.

### 5.5 Arquitectura de Software del Gateway

El presente capítulo se enfoca en el **Nivel 3 (Gateway IoT)**, desarrollando en profundidad su arquitectura de software, hardware, configuración y despliegue. Los niveles 1 y 2 se mencionan cuando sea necesario para contextualizar la integración.

#### 5.5.1 Stack de Contenedores

El gateway implementa una arquitectura basada en contenedores Docker con servicios desacoplados:

**Figura 5-2:** Arquitectura de contenedores del gateway OpenWRT

### Capa de Sistema Operativo (OpenWRT)

- **Kernel Linux 5.15+:** Con soporte para namespaces, cgroups y overlay filesystem.
- **UCI (Unified Configuration Interface):** Gestión centralizada de red, firewall y servicios.
- **nftables:** Firewall con reglas para aislamiento de contenedores y NAT.
- **netifd:** Gestión de interfaces de red (WAN, LAN, VLANs, bridges).

### Capa de Orquestación (Docker + Compose)

- **Docker Engine 24+:** Runtime de contenedores con storage driver overlay2.
- **Docker Compose 2.x:** Definición declarativa de multi-contenedor con volúmenes y redes.
- **LuCI Docker Manager:** Interfaz web para gestión visual de contenedores.

### Capa de Servicios (Contenedores)

- **OpenThread Border Router:** Gestión de red Thread y ruteo IPv6.
- **ThingsBoard Edge:** Plataforma IoT local con dashboards y reglas.
- **PostgreSQL:** Base de datos para persistencia de TB Edge.
- **Thread-TB Bridge:** Aplicación custom para integración OTBR ↔ TB Edge.
- **MQTT Broker (Mosquitto):** Opcional, para separar tráfico interno.

## 5.5.2 Stack de Comunicación

### Capa Física y de Enlace

- **802.15.4/Thread:** Interfaz radio RCP (nRF52840/ESP32-H2) conectada vía USB al contenedor OTBR.
- **802.11ah (HaLow - Morse Micro):** Backhaul desde DCUs al gateway (902-928 MHz, hasta 3 km).
- **802.11ac/ax:** WiFi dual-band (2.4/5 GHz) para gestión local y configuración web.
- **LTE Cat-6 (M.2):** Uplink celular para zonas sin infraestructura fija o como backup WAN.
- **Ethernet Gigabit:** Puerto WAN para fibra/ADSL/cable como uplink primario + 4 puertos LAN.

### Diagrama de conectividad:

DCUs (Thread)

↓ [802.11ah / Morse Micro / 902-928 MHz / hasta 3 km]

Gateway OpenWRT (HaLow AP + OTBR + TB Edge)

↓ [WAN: Ethernet Gigabit (prioridad 1) o LTE M.2 (prioridad 2)]

Internet → ThingsBoard Cloud

## Capa de Red

- **IPv6:** Red Thread usa prefijo ULA `fd00::/64`, ruteado por OTBR hacia LAN.
- **IPv4 NAT:** Para uplink WAN hacia Internet y ThingsBoard Cloud.
- **mDNS/DNS-SD:** Descubrimiento de servicios entre Thread y LAN (proxy en OTBR).

## Capa de Transporte

- **TCP/TLS:** Conexiones seguras entre TB Edge y ThingsBoard Cloud (puerto 7070).
- **MQTT/TLS:** Publicación de telemetría desde bridge hacia TB Edge (puerto 1883/8883).
- **CoAP/UDP:** Protocolo ligero para dispositivos Thread con recursos limitados.

## Capa de Aplicación

- **MQTT 3.1.1/5.0:** Protocolo principal para telemetría y comandos.
- **HTTP/REST:** API de TB Edge para configuración y consultas.
- **WebSocket:** Para dashboards en tiempo real en interfaz web de TB Edge.
- **JSON:** Formato de serialización estándar para payloads.

### 5.5.3 Componentes de Software

#### Contenedor OpenThread Border Router

Responsable de:

- Gestionar la red Thread (formación, comisionado, ruteo).
- Actuar como líder (Leader) de la red Thread mesh.
- Rutear tráfico IPv6 entre Thread (`fd00::/64`) y LAN.
- Proporcionar web UI para diagnóstico y configuración ([http://\[fd00::1\]:80](http://[fd00::1]:80)).
- Publicar prefijos de red vía Router Advertisement.

Configuración de red Thread:

```
docker exec -it otbr ot-ctl dataset init new
docker exec -it otbr ot-ctl dataset networkname "SmartGrid-Thread"
docker exec -it otbr ot-ctl dataset panid 0xABCD
docker exec -it otbr ot-ctl dataset channel 15
docker exec -it otbr ot-ctl dataset commit active
docker exec -it otbr ot-ctl ifconfig up
docker exec -it otbr ot-ctl thread start
```

## Contenedor ThingsBoard Edge

Funciones principales:

- **Ingestión de datos:** Recibe telemetría vía MQTT, HTTP, CoAP desde bridge.
- **Procesamiento local:** Ejecuta reglas (Rule Engine) para alarmas y transformaciones.
- **Almacenamiento:** Persiste time-series en PostgreSQL local.
- **Dashboards:** Interfaz web con visualizaciones en tiempo real.
- **Sincronización cloud:** Envía datos agregados a ThingsBoard Cloud vía gRPC.

Creación de dispositivo en TB Edge:

```
# Vía API REST
curl -X POST http://localhost:8080/api/device \
-H "X-Authorization: Bearer $TOKEN" \
-d '{
    "name": "SmartMeter-001",
    "type": "energy-meter",
    "label": "Medidor Residencial Sector A"
}'
```

## Contenedor PostgreSQL

- Base de datos relacional para TB Edge (dispositivos, usuarios, dashboards).
- Time-series híbrido con extensión TimescaleDB (opcional, mejora rendimiento).
- Volumen persistente en /mnt/docker/postgres-data para sobrevivir reinicios.
- Backups automáticos vía cron: pg\_dump diario a /mnt/docker/backups.

## Bridge Thread ↔ ThingsBoard

Aplicación custom (Python/Node.js) que:

- Suscribe a topics MQTT de dispositivos Thread (publicados localmente).
- Parsea payloads (CBOR/JSON) y extrae telemetría (energía, potencia, voltaje).
- Transforma a formato ThingsBoard:

```
{
  "ts": 1730000000000,
  "values": {
    "energy_kwh": 1234.56,
    "power_w": 3450.0,
    "voltage_v": 220.5,
    "current_a": 15.68,
    "frequency_hz": 60.02
  }
}
```

- Publica a TB Edge vía MQTT usando access token del dispositivo.
- Maneja reconexión, buffering local (Redis/SQLite) en caso de downtime de TB Edge.

Ejemplo de implementación (Node.js):

```
const mqtt = require('mqtt');

// Cliente para Thread devices
const threadClient = mqtt.connect('mqtt://localhost:1883');

// Cliente para TB Edge
const tbClient = mqtt.connect('mqtt://localhost:1883', {
  username: 'DEVICE_ACCESS_TOKEN'
});

threadClient.on('message', (topic, payload) => {
  const data = JSON.parse(payload);

  const telemetry = {
    ts: Date.now(),
    values: {
      energy_kwh: data.energy,
      power_w: data.power,
      voltage_v: data.voltage
    }
  };

  tbClient.publish('v1/devices/me/telemetry',
    JSON.stringify(telemetry));
});

threadClient.subscribe('thread/telemetry/#');
```

## Módulo de Seguridad

- **Firewall nftables:** Reglas para aceptar solo puertos necesarios (MQTT 1883/8883, HTTP 8080, SSH 22).
- **TLS/mTLS:** Certificados X.509 para conexión TB Edge ↔ TB Cloud.
- **Secrets management:** Variables sensibles (passwords, tokens) en Docker secrets o variables de entorno cifradas.
- **Actualizaciones automáticas:** Watchtower container para actualizar imágenes Docker periódicamente.

Ejemplo de reglas nftables:

```
# Permitir MQTT desde LAN a contenedores
nft add rule inet fw4 forward iifname "br-lan" \
    tcp dport {1883, 8883} accept

# Bloquear acceso externo a PostgreSQL
nft add rule inet fw4 input iifname "wan" \
    tcp dport 5432 drop
```

## 5.6 Flujo de Datos End-to-End

### 5.6.1 Flujo Normal de Operación

1. **Medidor → Nodo Thread (ESP32C6):** El medidor inteligente envía lecturas vía RS-485/DLMS al nodo adaptador Thread.
2. **Nodo Thread → OTBR:** El nodo publica telemetría vía CoAP/MQTT sobre Thread (IPv6 fd00::/64).
3. **OTBR: Ruteo IPv6:** El contenedor OTBR rutea el paquete desde Thread hacia la red LAN del gateway.
4. **Bridge: Transformación:** El contenedor bridge recibe el mensaje, lo parsea y transforma al formato ThingsBoard.
5. **Bridge → TB Edge:** El bridge publica vía MQTT (puerto 1883) al contenedor TB Edge.
6. **TB Edge: Procesamiento:** TB Edge ejecuta Rule Engine (ej. alarmas por consumo excesivo), actualiza dashboards y almacena en PostgreSQL.
7. **TB Edge → TB Cloud:** Periódicamente (cada 5 min), TB Edge sincroniza datos agregados con ThingsBoard Cloud vía gRPC/TLS (puerto 7070).
8. **Usuario: Visualización:** Operador accede a dashboards en TB Cloud o localmente en TB Edge (<http://<gateway-ip>:8080>).

### 5.6.2 Flujo en Modo Edge (Sin Conectividad Cloud)

1. Gateway detecta pérdida de conectividad WAN (ping a 8.8.8.8 falla).
2. TB Edge activa modo offline: continúa recibiendo telemetría local y ejecutando reglas.
3. Dashboards locales permanecen funcionales (acceso vía LAN).
4. Datos se acumulan en PostgreSQL local (límite: 30 días o 10 GB, configurable).
5. Al recuperar conectividad, TB Edge sincroniza automáticamente backlog con cloud (chunked uploads).

### 5.6.3 Flujo de Comandos Downlink (Cloud → Dispositivo)

1. Operador envía comando desde TB Cloud (ej. cambiar intervalo de lectura a 5 min").
2. TB Cloud envía comando a TB Edge vía gRPC.
3. TB Edge publica comando en topic MQTT: v1/devices/<device-id>/rpc/request/+.
4. Bridge suscrito a este topic recibe el comando y lo traduce al formato Thread/CoAP.
5. Bridge envía comando CoAP PUT a dispositivo Thread: coap://[fd00::abcd]/config/interval.
6. Dispositivo Thread ejecuta comando, responde con ACK y actualiza configuración.
7. Bridge publica respuesta a TB Edge: v1/devices/<device-id>/rpc/response/123.
8. TB Edge sincroniza respuesta con TB Cloud.

### 5.6.4 Flujo de Actualización OTA de Contenedores

1. Watchtower container verifica actualizaciones de imágenes Docker cada 24h.
2. Si nueva versión disponible (ej. openthread/otbr:3.5.0), descarga imagen.
3. Watchtower detiene contenedor actual, crea nuevo con misma configuración (volúmenes, redes).
4. Si nuevo contenedor arranca correctamente (healthcheck OK), elimina imagen antigua.
5. Si falla, rollback automático a imagen anterior.
6. Logs de actualización en /mnt/docker/watchtower/watchtower.log.

## 5.7 Implementación del Gateway con OpenWRT

### 5.7.1 Justificación de la Plataforma

Se selecciona OpenWRT como sistema operativo del gateway por:

- **Flexibilidad:** Linux embebido con gestión de paquetes (opkg) y configuración vía UCI.
- **Sohorte Docker:** Contenedorización de servicios (OpenThread Border Router, ThingsBoard Edge).
- **Redes avanzadas:** VLAN, firewall (nftables), QoS, IPv6 nativo.
- **Hardware compatible:** Amplio soporte para routers con expansión de almacenamiento (USB, NVMe).
- **Comunidad activa:** Actualizaciones de seguridad frecuentes y extenso repositorio de paquetes.

### 5.7.2 Hardware del Gateway

#### Plataforma Base

- **SoC:** MediaTek MT7621AT (MIPS 1004Kc dual-core @ 880 MHz) o similar con soporte PCIe y M.2.
- **RAM:** 512 MB DDR3 para soportar Docker y múltiples contenedores simultáneos.
- **Flash:** 16 MB NOR flash para OpenWRT + 32 GB USB 3.0/NVMe M.2 para contenedores y datos.
- **WiFi dual-band:** 802.11ac/ax (2.4/5 GHz) para gestión y configuración local.
- **Ethernet:** 5 puertos Gigabit (1 WAN + 4 LAN) con soporte PoE+ para alimentación.
- **Alimentación:** PoE+ 802.3at (25W) o adaptador 12V/2A.

#### Conectividad 802.11ah (HaLow) con Morse Micro

El gateway integra chipset **Morse Micro MM6108** para comunicación HaLow:

- **Chipset:** Morse Micro MM6108 SoC con soporte 802.11ah completo.
- **Interfaz:** PCIe/SDIO conectado al bus del router vía miniPCIe o M.2 Key E.
- **Frecuencia:** 902-928 MHz (ISM band, región América) con canales de 1/2/4/8 MHz.
- **Alcance:** Hasta 1-3 km en línea de vista con antena externa 5 dBi.
- **Throughput:** Hasta 40 Mbps (MCS10, 8 MHz BW) suficiente para 10+ DCUs.
- **Seguridad:** WPA3-SAE con PMF (Protected Management Frames) obligatorio.
- **Ventajas Morse Micro:**
  - Estabilidad industrial: operación -40°C a +85°C.
  - Drivers Linux mainline (ath11k) con soporte OpenWRT nativo.
  - Menor consumo: <500 mW en TX, <50 mW en RX.
  - Certificaciones FCC/CE completadas para despliegue comercial.

#### Modos de Operación HaLow Soportados:

- **AP (Access Point)**: Gateway como punto de acceso central para DCUs.
- **STA (Station)**: Gateway como cliente conectado a AP HaLow externo.
- **802.11s Mesh**: Malla autogestionada entre múltiples gateways.
- **EasyMesh**: IEEE 1905.1 con Multi-AP para roaming y gestión centralizada.

## 5.8 Implementación en Raspberry Pi 4 con OpenWRT

### 5.8.1 Hardware de la Implementación Real

#### Plataforma Raspberry Pi 4 Model B

El prototipo del gateway se implementó sobre **Raspberry Pi 4 Model B** debido a sus capacidades superiores de procesamiento multi-core y memoria RAM, esenciales para ejecutar múltiples contenedores Docker simultáneamente.

#### Especificaciones Raspberry Pi 4:

- **SoC**: Broadcom BCM2711, Cortex-A72 quad-core ARMv8 64-bit @ 1.5 GHz
- **RAM**: 4 GB LPDDR4-3200 SDRAM (versión 4 GB seleccionada)
- **GPU**: VideoCore VI @ 500 MHz (OpenGL ES 3.1, Vulkan 1.0)
- **Almacenamiento**:
  - Boot: microSD 32 GB Class 10 (OpenWRT system)
  - Data: M.2 NVMe SSD 256 GB via PCIe HAT (Docker volumes, PostgreSQL, queue)
- **Conectividad integrada**:
  - Ethernet: Gigabit Ethernet (1000 Mbps, Broadcom BCM54213PE PHY)
  - WiFi: 802.11ac dual-band 2.4/5 GHz (Cypress CYW43455, usado solo para gestión local)
  - Bluetooth: 5.0 BLE (no utilizado en esta implementación)
- **Puertos de expansión**:
  - 2× USB 3.0 (5 Gbps)
  - 2× USB 2.0 (480 Mbps)
  - 40-pin GPIO header (alimentación 3.3V/5V, I2C, SPI, UART)
  - 1× PCIe 1× lane via GPIO 40-pin (requiere HAT adapter)
- **Alimentación**: 5V/3A via USB-C (fuente oficial Raspberry Pi)
- **Dimensiones**: 85 mm × 56 mm × 17 mm (sin HATs)
- **Consumo típico**: 2.7-6.4W según carga (idle vs CPU 100%)

Característica	RPi 4 (BCM2711)	Router MT7621AT
Arquitectura CPU	ARMv8 64-bit	MIPS 1004Kc 32-bit
Cores	4 (Cortex-A72)	2 (880 MHz)
Clock	1.5 GHz	880 MHz
RAM	4 GB LPDDR4	512 MB DDR3
Docker support	Nativo ARM64	Limitado (swap req.)
PostgreSQL	Sí (TimescaleDB ARM64)	No (insuf. RAM)
Kafka	Sí (Confluent ARM64)	No (OOM frecuente)
PCIe nativo	Sí (1x lane via HAT)	Sí (miniPCIe)
GPIO/SPI	40-pin, SPI0/1	Limitado
Costo (2025)	\$55 (4 GB)	\$40-60 (industrial)

Tabla 5-2: Comparación Raspberry Pi 4 vs Router OpenWRT tradicional

### Justificación de Raspberry Pi 4 vs Router OpenWRT Tradicional

#### Ventajas clave de Raspberry Pi 4 para este proyecto:

1. **Multi-core real:** 4 núcleos Cortex-A72 permiten paralelización de contenedores Docker (OTBR, TB Edge, PostgreSQL, Kafka) sin contención de CPU.
2. **RAM abundante:** 4 GB suficientes para PostgreSQL (512 MB), Kafka (1 GB), TB Edge (1 GB), sistema (500 MB) con margen.
3. **Ecosistema ARM64:** Imágenes Docker oficiales multi-arch (linux/arm64/v8) disponibles para todos los componentes.
4. **PCIe para NVMe:** M.2 HAT permite SSD NVMe con >3000 IOPS, crítico para PostgreSQL y queue persistente.
5. **GPIO/SPI flexible:** Conexión directa de módulo HaLow via SPI sin necesidad de adaptadores USB.
6. **Comunidad:** Soporte extendido de OpenWRT, drivers mainline, documentación abundante.

#### Desventajas (mitigadas):

- **No switch Ethernet integrado:** Solo 1 puerto Gigabit (suficiente para gateway con uplink único).
- **No PoE nativo:** Requiere HAT PoE+ (IEEE 802.3at) para alimentación centralizada (agregado en implementación).
- **Thermal throttling:** CPU reduce frecuencia si T° >80°C, mitigado con ventilador activo (ver sección térmica).

### Periféricos y Módulos de Conectividad

#### Thread/802.15.4: nRF52840 Dongle Hardware:

- **Modelo:** Nordic Semiconductor nRF52840 Dongle (PCA10059)
- **SoC:** nRF52840 (ARM Cortex-M4F @ 64 MHz, 1 MB Flash, 256 KB RAM)
- **Radio:** 802.15.4 @ 2.4 GHz, Bluetooth 5.3, Thread 1.3, Zigbee 3.0

- **Potencia TX:** +8 dBm máximo (configurable -20 a +8 dBm)
- **Sensibilidad RX:** -95 dBm (250 kbps OQPSK)
- **Interfaz:** USB 2.0 Full-Speed (conectado a USB 3.0 port de RPi 4)
- **Antena:** Integrada PCB 2.4 GHz (omnidireccional, ganancia 2 dBi)
- **Firmware:** OpenThread RCP (Radio Co-Processor) v1.3
- **Identificación en Linux:** /dev/ttyACM0 (CDC ACM device)

#### **Rol en arquitectura:**

- nRF52840 ejecuta stack 802.15.4 PHY/MAC en modo RCP.
- Raspberry Pi ejecuta OpenThread Border Router (OTBR) que controla RCP via UART over USB.
- Gateway expone prefijo Thread (fd00::/64) y rutea paquetes IPv6 entre Thread mesh y Ethernet/HaLow.

#### *HaLow 802.11ah: Morse Micro MM6108 via SPI    Hardware:*

- **Chipset:** Morse Micro MM6108 SoC
- **Estándar:** IEEE 802.11ah-2016 completo (S1G PHY)
- **Frecuencia:** 902-928 MHz (ISM band US/América)
- **Canales:** 1/2/4/8 MHz bandwidth (implementación usa 8 MHz)
- **Throughput:** Hasta 40 Mbps (MCS10, 8 MHz, MIMO 1×1)
- **Alcance típico:** 1-3 km LOS (line-of-sight) con antena 5 dBi
- **Potencia TX:** +20 dBm (100 mW, regulación FCC Part 15.247)
- **Consumo:** <500 mW TX, <50 mW RX, <10 mW sleep
- **Interfaz Raspberry Pi:** SPI0 via GPIO 40-pin
  - GPIO 8 (CE0): Chip Select
  - GPIO 10 (MOSI): Master Out Slave In
  - GPIO 9 (MISO): Master In Slave Out
  - GPIO 11 (SCLK): SPI Clock (max 10 MHz)
  - GPIO 25: Interrupt Request (IRQ)
- **Driver Linux:** ath11k (mainline kernel 5.19+, backport a OpenWRT 23.05)
- **Identificación:** wlan2 (wireless interface)
- **Roadmap:** Soporte USB 2.0 High-Speed planificado (Q2 2026) para simplificar integración en futuras versiones.

#### **Conexión SPI en GPIO Raspberry Pi 4:**

```
# Pines físicos en GPIO 40-pin header
Pin 19 (GPIO 10) --> MOSI      (Morse Micro)
Pin 21 (GPIO 9)   --> MISO      (Morse Micro)
Pin 23 (GPIO 11) --> SCLK      (Morse Micro)
Pin 24 (GPIO 8)   --> CS0       (Morse Micro)
Pin 22 (GPIO 25) --> IRQ        (Morse Micro)
Pin 17             --> 3.3V     (alimentación módulo)
Pin 20             --> GND       (ground común)
```

#### Habilitación SPI en OpenWRT:

```
# /boot/config.txt (Raspberry Pi firmware config)
dtparam=spi=on
dtoverlay=spi0-1cs

# Verificar dispositivo SPI
ls -l /dev/spidev0.0
# Esperado: crw-rw---- 1 root spi 153, 0 /dev/spidev0.0

# Cargar módulo ath11k_ahb (AHB bus para SPI)
modprobe ath11k_ahb

# Verificar interfaz wireless
iw dev
# Esperado: wlan2 Interface phy#2 type managed
```

#### LTE Modem: Quectel BG95-M3 Hardware:

- **Modelo:** Quectel BG95-M3 (LTE Cat-M1/Cat-NB2 + EGPRS)
- **Bandas LTE-M (Cat-M1):** B2/B4/B5/B12/B13 (cobertura América)
- **Bandas NB-IoT (Cat-NB2):** B2/B4/B5/B12/B13/B66/B71
- **Fallback:** EGPRS (2G) para zonas sin LTE
- **Throughput:** 375 kbps DL / 375 kbps UL (Cat-M1), 60 kbps (NB-IoT)
- **Latencia:** 100-300 ms (Cat-M1), 1-10 s (NB-IoT)
- **Interfaz:** USB 2.0 High-Speed (conectado a USB 3.0 port de RPi 4)
- **Protocolo:** QMI (Qualcomm MSM Interface) + AT commands
- **GNSS integrado:** GPS/GLONASS/Galileo/BeiDou (no utilizado en gateway)
- **SIM:** Nano-SIM (4FF) con plan M2M de operador local
- **Antena:** Externa 4G/LTE 3 dBi (conector U.FL/IPEX)
- **Consumo:** <300 mA @ 3.3V (1W típico), <10 mA PSM (Power Save Mode)
- **Certificaciones:** FCC/CE/PTCRB/GCF (aprobado operadores América)

#### Identificación en Linux:

```
# USB device
lsusb | grep Quectel
# Esperado: Bus 001 Device 004: ID 2c7c:0296 Quectel Wireless Solutions Co.

# Interfaces de red
ls /dev/ttyUSB*
# /dev/ttyUSB0 (AT commands)
# /dev/ttyUSB1 (PPP dial-up, no usado)
# /dev/ttyUSB2 (NMEA GPS, no usado)

# QMI network interface (usado para data)
ls /sys/class/net/
# wwan0 (QMI interface)
```

#### Ventajas Quectel BG95 para Smart Energy:

- **LTE-M optimizado:** Menor latencia vs NB-IoT (100 ms vs 1-10 s), adecuado para comandos RPC downlink.
- **Bajo consumo:** PSM mode permite <10 mA idle, extendiendo operación con baterías de respaldo.
- **Multi-band:** Cobertura Colombia (B2/B4), México (B2/B4/B5), USA (B12/B13).
- **Fallback 2G:** EGPRS garantiza conectividad en zonas rurales sin LTE.
- **Drivers mainline:** ModemManager + QMI support nativo en OpenWRT 23.05.

#### *Almacenamiento: M.2 NVMe SSD via PCIe HAT Hardware:*

- **HAT:** Geekworm X1001 M.2 NVMe PCIe HAT
- **Interfaz:** PCIe 1× Gen 2 (5 Gbps, 500 MB/s teórico)
- **Conexión:** GPIO 40-pin (PCIe lanes redirigidos desde USB 3.0 controller)
- **SSD:** Kingston NV2 M.2 2280 NVMe 256 GB (PCIe 4.0, retrocompatible PCIe 2.0)
- **Performance medida** (con Raspberry Pi 4 PCIe 2.0):
  - Lectura secuencial: 350-400 MB/s
  - Escritura secuencial: 280-320 MB/s
  - IOPS 4K random read: 3200-3500
  - IOPS 4K random write: 2800-3200
  - Latencia: <1 ms (95th percentile)
- **Filesystem:** ext4 con journaling, montado en /mnt/ssd
- **Uso:**
  - /mnt/ssd/docker/ (Docker data root, 100 GB)
  - /mnt/ssd/postgres/ (PostgreSQL + TimescaleDB, 80 GB)
  - /mnt/ssd/tb-edge-data/ (ThingsBoard Edge queue, 50 GB)
  - /mnt/ssd/backups/ (backups automáticos, 26 GB)

#### Ventajas NVMe vs microSD/USB:

Métrica	microSD Class 10	USB 3.0 SSD	NVMe M.2 (HAT)
Lectura seq. (MB/s)	80-95	250-400	350-400
Escritura seq. (MB/s)	20-40	200-350	280-320
IOPS 4K random	100-500	1000-2000	3000-3500
Latencia (ms)	5-20	1-5	<1
Durabilidad (ciclos E/W)	10k-100k	100k-1M	>1M
MTBF (horas)	50k	1M	1.5M

Tabla 5-3: Comparación almacenamiento para gateway IoT

**Alimentación: PoE+ HAT Hardware:**

- **Modelo:** Waveshare PoE HAT (B) for Raspberry Pi 4
- **Estándar:** IEEE 802.3at (PoE+, 25.5W máx)
- **Entrada:** 42-57V DC (inyector PoE en switch Ethernet)
- **Salida:** 5V/5A (25W) via GPIO 40-pin
- **Eficiencia:** >85 % (típico 90 %)
- **Ventilador:** 30 mm, 5V, control PWM por GPIO (encendido si T°>60°C)
- **Aislamiento:** 1500V DC isolation

**Ventajas PoE+ para gateway Smart Energy:**

- Instalación simplificada: 1 cable Ethernet (datos + alimentación).
- Redundancia: UPS centralizado en switch PoE mantiene gateway operativo ante corte eléctrico.
- Cable >50m: Cat5e/Cat6 sin degradación (vs USB-C limitado a 1-2m).

**5.8.2 Sistema Operativo: OpenWRT 23.05 en Raspberry Pi 4****Versión y Arquitectura**

- **Versión OpenWRT:** 23.05.0 (released 2023-10)
- **Target:** bcm27xx/bcm2711 (Raspberry Pi 4 specific)
- **Subtarget:** rpi-4 (64-bit ARMv8 kernel)
- **Kernel:** Linux 5.15.134 (LTS kernel con patches Raspberry Pi Foundation)
- **Arquitectura binarios:** aarch64\_cortex-a72 (ARM64v8)
- **Libc:** musl 1.2.4 (lightweight C library)
- **Bootloader:** Raspberry Pi firmware (start4.elf, bootcode.bin en FAT32 boot partition)

---

Instalación OpenWRT en Raspberry Pi 4**Paso 1: Descarga de imagen:**

```
# Descargar imagen oficial desde OpenWRT
wget https://downloads.openwrt.org/releases/23.05.0/targets/bcm27xx/bcm2711/\
openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img.gz

# Verificar checksum SHA256
sha256sum openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img.gz
```

**Paso 2: Escritura en microSD:**

```
# Linux/macOS
gunzip openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img.gz
sudo dd if=openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img \
      of=/dev/sdX bs=4M conv=fsync status=progress
# Reemplazar /dev/sdX con dispositivo correcto (lsblk para listar)

# Windows: usar Raspberry Pi Imager o balenaEtcher
# Seleccionar imagen .img y microSD target
```

**Paso 3: Configuración inicial (first boot):**

```
# Conectar RPi 4 a red Ethernet (DHCP automático en eth0)
# Conectar via SSH (default IP: 192.168.1.1 si no DHCP)
ssh root@192.168.1.1
# Password inicial: <vacío> (presionar Enter)

# Cambiar password root
passwd
# Ingresar nueva contraseña segura

# Configurar hostname
uci set system.@system[0].hostname='smartgrid-gateway-001'
uci commit system
/etc/init.d/system reload

# Actualizar timezone
uci set system.@system[0].timezone='CST6CDT,M3.2.0,M11.1.0'  # Colombia
uci set system.@system[0].zonename='America/Bogota'
uci commit system
/etc/init.d/system reload

# Configurar NTP servers
uci set system.ntp.server='0.co.pool.ntp.org'
uci add_list system.ntp.server='1.co.pool.ntp.org'
uci commit system
/etc/init.d/sysntpd restart
```

**Paso 4: Actualización de paquetes y drivers esenciales:**

```
# Actualizar lista de paquetes
opkg update

# Instalar utilidades base
opkg install nano htop iperf3 tcpdump curl wget-ssl ca-certificates

# Docker y dependencias
opkg install dockerd docker-compose luci-app-dockerman
opkg install kmod-nf-nat kmod-veth kmod-br-netfilter

# ModemManager para Quectel BG95
opkg install modemmanager libqmi usb-modeswitch

# OpenThread Border Router dependencies
opkg install wpantund ot-br-posix avahi-daemon

# HaLow drivers (ath11k backport)
opkg install kmod-ath11k kmod-ath11k-ahb

# SPI support
opkg install kmod-spi-bcm2835 kmod-spi-dev

# Filesystem tools
opkg install e2fsprogs fdisk blkid kmod-usb-storage kmod-fs-ext4
```

## Configuración de Almacenamiento NVMe

### Detección y particionamiento:

```
# Verificar detección de SSD NVMe
lsblk
# Esperado:
# nvme0n1      259:0    0 238.5G  0 disk
# nvme0n1p1  259:1    0 238.5G  0 part

# Si no particionado, crear partición GPT
fdisk /dev/nvme0n1
# Comandos: g (create GPT), n (new partition), w (write)

# Formatear ext4 con journaling
mkfs.ext4 -L ssd-data /dev/nvme0n1p1

# Crear punto de montaje
mkdir -p /mnt/ssd

# Montaje automático en /etc/config/fstab
block detect > /etc/config/fstab
uci set fstab.@mount[-1].enabled='1'
uci set fstab.@mount[-1].target='/mnt/ssd'
uci commit fstab
/etc/init.d/fstab enable
/etc/init.d/fstab start
```

```
# Verificar montaje
df -h /mnt/ssd
# Esperado: /dev/nvme0n1p1 234G 60M 222G 1% /mnt/ssd

# Crear directorios Docker
mkdir -p /mnt/ssd/docker
mkdir -p /mnt/ssd/postgres
mkdir -p /mnt/ssd/tb-edge-data
mkdir -p /mnt/ssd/backups
```

#### Configuración Docker data-root en SSD:

```
# /etc/docker/daemon.json
{
  "data-root": "/mnt/ssd/docker",
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "10m",
    "max-file": "3"
  },
  "storage-driver": "overlay2"
}

# Reiniciar Docker
/etc/init.d/dockerd restart

# Verificar data-root
docker info | grep "Docker Root Dir"
# Esperado: Docker Root Dir: /mnt/ssd/docker
```

### 5.8.3 Configuración de Conectividad

#### 5.8.4 Configuración de Conectividad

El gateway integra múltiples interfaces de red mediante configuraciones UCI (Unified Configuration Interface) de OpenWRT:

- **Thread 802.15.4:** OpenThread Border Router (OTBR) con nRF52840 RCP via USB (`/dev/ttyACM0`), forma red **SmartGrid-Thread** en canal 15
- **HaLow 802.11ah:** Tarjeta MM6108 via SPI, soporta 4 modos (AP Router, STA Client, Mesh 802.11s, EasyMesh 1905.1)
- **LTE Cat-M1/NB-IoT:** Quectel BG95-M3 via USB, gestionado por ModemManager, interfaz `wwan0` con failover vía `mwan3`
- **Ethernet Gigabit:** `eth0` como WAN primaria, enlace 1000BASE-T a ISP o red corporativa

Las configuraciones UCI completas para HaLow en sus cuatro modos de operación (AP Router con NAT, STA Client, Mesh 802.11s, EasyMesh 1905.1 Controller/Agent) se presentan en el Anexo D. Los comandos de inicialización de OTBR y LTE modem se documentan en el Anexo B con los docker-compose correspondientes.

Ejemplo de verificación de interfaces activas:

```
# Thread Border Router
docker exec otbr ot-ctl state
# Esperado: "leader" o "router" (red Thread activa)

# HaLow 802.11ah
iw dev wlan2 info
# Esperado: Interface wlan2, type AP, channel 7 (917 MHz)

# LTE modem
mmcli -m 0 --simple-status
# Esperado: state: connected, signal-quality: 75%

# Ethernet WAN
cat /sys/class/net/eth0/operstate
# Esperado: up (enlace 1000BASE-T activo)
```

```
uci set wireless.halow_ap.ieee80211w='2' PMF required reduce wireless.halow_ap.max_inactivity='600' mintimeout uci set wireless.halow_ap.ieee80211w='10' 10mintimeout uci set wireless.halow_ap.ieee80211w='10' 10mintimeout
```

Red independiente con NAT uci set network.halowlan = interface ucisetnetwork.halowlan.proto = ' static' ucisetnetwork.halowlan.ip4 = 192.168.50.1 ucisetnetwork.halowlan.netmask = ' 255.255.255.0' ucicommitnetwork wireless/etc/init.d/network restart wifi

### Configuración Bridge Mode (L2)

```
# HaLow AP bridged a br-lan
uci set wireless.hallow_ap.network='lan'
uci set wireless.hallow_ap.mode='ap'
uci delete network.hallow_lan # No red separada
uci commit
wifi reload
```

## Ventajas:

- Cobertura centralizada: DCUs hasta 3 km LOS.
  - Control total: airtime fairness, QoS, filtrado MAC.
  - Simplicidad: topología estrella sin routing complejo.

### Desventajas:

- Single point of failure.
- No extensión automática de rango.

**Modo STA (Station/Cliente)** **Función:** Gateway se conecta como cliente a un AP HaLow externo (ej. backhaul rural).

#### Configuración:

```
uci set wireless.hallow_sta=wifi-iface
uci set wireless.hallow_sta.device='halow'
uci set wireless.hallow_sta.mode='sta'
uci set wireless.hallow_sta.network='wan' # Uplink WAN
uci set wireless.hallow_sta.ssid='Utility-HaLow-Backhaul'
uci set wireless.hallow_sta.encryption='sae'
uci set wireless.hallow_sta.key='<WPA3-KEY>'
uci set wireless.hallow_sta.ieee80211w='2'
uci commit wireless
wifi reload
```

**Caso de uso:** Gateway en zona rural sin fibra/LTE, conecta vía HaLow a torre de utilidad con enlace backhaul.

#### Ventajas:

- Ahorro costo celular (sin plan LTE mensual).
- Mayor throughput que LTE en zonas congestionadas.

**Modo 802.11s Mesh** **Función:** Malla autogestionada entre múltiples gateways HaLow con routing automático.

#### Configuración:

```
# Instalar paquete mesh
opkg install wpad-mesh-openssl

uci set wireless.hallow_mesh=wifi-iface
uci set wireless.hallow_mesh.device='halow'
uci set wireless.hallow_mesh.mode='mesh'
uci set wireless.hallow_mesh.mesh_id='SmartGrid-Mesh'
uci set wireless.hallow_mesh.network='mesh_lan'
uci set wireless.hallow_mesh.encryption='sae'
uci set wireless.hallow_mesh.key='<MESH-KEY>'
```

```

uci set wireless.halow_mesh.mesh_fwding='1'
uci set wireless.halow_mesh.mesh_ttl='31'

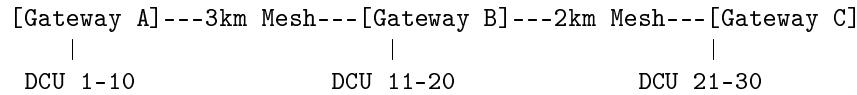
# Red mesh con batman-adv
uci set network.mesh_lan=interface
uci set network.mesh_lan.proto='batadv_hardif'
uci set network.mesh_lan.master='bat0'
uci set network.mesh_lan.mtu='1532'

uci set network.bat0=interface
uci set network.bat0.proto='static'
uci set network.bat0.ipaddr='10.50.0.1'
uci set network.bat0.netmask='255.255.255.0'
uci commit
/etc/init.d/network restart
wifi reload

```

**Protocolo de routing:** HWMP (Hybrid Wireless Mesh Protocol) en kernel o batman-adv en userspace.

#### Arquitectura extendida:



#### Ventajas:

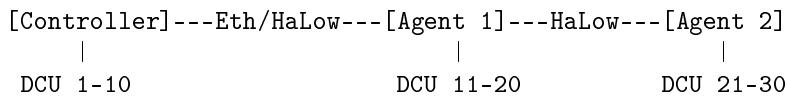
- Auto-healing: rutas alternativas si un nodo falla.
- Extensión de cobertura: 3 gateways = 6-9 km total.
- Sin infraestructura central.

#### Desventajas:

- Latencia variable (multi-hop).
- Overhead de protocolo mesh (15-20 % throughput).

**Modo EasyMesh (IEEE 1905.1 Multi-AP)** Función: Controller/Agent mesh con gestión centralizada y roaming WiFi entre APs.

#### Arquitectura:

**Configuración Controller:**

```

opkg install ieee1905-daemon map-controller

# Controller config
uci set mapcontroller.config=config
uci set mapcontroller.config.enabled='1'
uci set mapcontroller.config.interfaces='eth0 wlan2'
uci commit mapcontroller
/etc/init.d/ieee1905 restart

# HaLow AP frontal
uci set wireless.hallow_ap.easymesh='1'
uci commit wireless
wifi reload
  
```

**Configuración Agent:**

```

opkg install ieee1905-daemon map-agent

uci set mapagent.config=config
uci set mapagent.config.enabled='1'
uci set mapagent.config.controller='192.168.1.1'
uci set mapagent.config.backhaul_iface='wlan2' # HaLow backhaul
uci commit mapagent
/etc/init.d/ieee1905 restart
  
```

**Ventajas:**

- Roaming transparente: DCU cambia entre APs sin desconexión.
- Gestión centralizada: configuración desde Controller.
- Steering: Controller dirige clientes a AP óptimo (load balancing).
- Band steering: 802.11ah + 802.11n/ac combinados.

**Desventajas:**

- Complejidad: requiere IEEE 1905.1 daemon.
- Controller single point of failure (mitigar con HA).

Característica	AP	STA	802.11s Mesh	EasyMesh
Cobertura	3 km	3 km	6-9 km	6-9 km
Topología	Estrella	P2P	Malla	Árbol
Auto-healing	No	No	Sí	Sí
Roaming	No	N/A	Manual	Automático
Gestión	Local	N/A	Distribuida	Centralizada
Complejidad	Baja	Baja	Media	Alta
Latencia	<50 ms	<50 ms	<200 ms	<100 ms
Throughput (10 nodos)	40 Mbps	40 Mbps	30 Mbps	35 Mbps

Tabla 5-4: Comparación de modos de operación HaLow

*Comparación de Modos HaLow*

*Recomendación de Arquitectura* Para despliegue de infraestructuras Smart Grid se recomienda:

- **Zona urbana densa (<1 km):** Modo AP con bridge a LAN.
- **Zona rural extendida (3-9 km):** Modo 802.11s Mesh con 2-3 gateways.
- **Multi-edificio (campus):** EasyMesh con Controller central y Agents por edificio.
- **Backup WAN:** Modo STA conectado a torre utilidad con fibra.

**Beneficios arquitectónicos de modos avanzados:**

1. **Extensión de cobertura:** Mesh/EasyMesh multiplica alcance sin infraestructura adicional (3 gateways = 9 km vs 3 km de AP único).
2. **Resiliencia:** Rutas alternativas en mesh eliminan single point of failure.
3. **Escalabilidad:** EasyMesh permite agregar Agents sin reconfigurar red completa.
4. **Reducción CAPEX:** Menos gateways con backhaul dedicado (fibra/LTE) al usar mesh HaLow como backhaul.
5. **QoE mejorada:** Roaming EasyMesh evita desconexiones durante handoff de DCU móvil (ej. vehículo de mantenimiento).

**Conectividad Celular LTE (M.2 Socket)**

Para redundancia y uplink WAN, el gateway incorpora módulo LTE Cat-4/Cat-6:

- **Socket:** M.2 Key B (PCIe + USB 3.0 combo) para módems 4G/LTE.
- **Módulos compatibles:**

- Quectel EM060K-GL (Cat-6, 300 Mbps DL, 50 Mbps UL).
  - Sierra Wireless EM7565 (Cat-12, 600 Mbps DL).
  - Telit LM960 (Cat-18, 1.2 Gbps DL con agregación de portadoras).
- **Bandas soportadas:** B2/B4/B5/B7/B12/B13/B66 (Colombia/Latinoamérica).
- **Interfaz:** USB 3.0 con protocolo QMI/MBIM, drivers ModemManager en OpenWRT.
- **SIM:** Nano-SIM con soporte eSIM (MFF2) en módulos avanzados.
- **Antenas:** 2x conectores U.FL para diversidad MIMO 2×2.
- **Consumo:** <2W en transmisión activa, <100mW en idle.
- **Casos de uso:**
- Uplink principal en zonas sin fibra/ADSL disponible.
  - Backup automático si falla conexión Ethernet WAN.
  - VPN site-to-site con ThingsBoard Cloud vía IPsec/WireGuard.

Configuración en OpenWRT (ModemManager):

```
opkg update
opkg install modemmanager luciproto-modemmanager usb-modeswitch

# Configurar interfaz LTE
uci set network.lte=interface
uci set network.lte.proto='modemmanager'
uci set network.lte.device='/sys/devices/platform/ahb/1e1c0000.xhci/usb1/1-1'
uci set network.lte.apn='internet.movistar.com.co'
uci set network.lte.pincode='0000'
uci set network.lte.metric='10' # Mayor prioridad que Ethernet WAN
uci commit network
ifup lte
```

Verificación de conexión:

```
mmcli -L # Listar módem detectados
mmcli -m 0 --simple-status # Estado (señal, operador, IP)
```

## Expansión de Almacenamiento

Para soportar Docker y volúmenes persistentes:

- **Opción 1:** USB 3.0 flash drive (32-64 GB) formateado ext4.

- **Opción 2:** Adaptador M.2 NVMe vía USB/PCIe (mejor rendimiento I/O).
- **Montaje:** /mnt/docker con overlay filesystem para /var/lib/docker.

Configuración en OpenWRT:

```
opkg update
opkg install block-mount kmod-fs-ext4 kmod-usb-storage-uas
mkfs.ext4 /dev/sda1
block detect > /etc/config/fstab
uci set fstab.@mount[0].target='/mnt/docker'
uci set fstab.@mount[0].enabled='1'
uci commit fstab
/etc/init.d/fstab enable
/etc/init.d/fstab start
```

### 5.8.5 Instalación de Docker en OpenWRT

#### Paquetes Requeridos

```
opkg install dockerd docker-compose luci-app-dockerman
/etc/init.d/dockerd enable
/etc/init.d/dockerd start
```

#### Configuración de Docker Daemon

Archivo /etc/docker/daemon.json:

```
{
  "data-root": "/mnt/docker",
  "storage-driver": "overlay2",
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "10m",
    "max-file": "3"
  }
}
```

Reiniciar Docker:

```
/etc/init.d/dockerd restart
docker info # Verificar data-root en /mnt/docker
```

## 5.8.6 Despliegue de OpenThread Border Router

### Función del OTBR

El OpenThread Border Router (OTBR) actúa como:

- **Puente IPv6**: Rutea tráfico entre red Thread (802.15.4) y backbone Ethernet/WiFi.
- **Comisionado Thread**: Permite unir nuevos dispositivos a la red Thread.
- **mDNS proxy**: Descubrimiento de servicios entre Thread e IP.
- **Web UI**: Interfaz de gestión en `http://[fd00::1]:80`.

### Docker Compose para OTBR

Archivo `/mnt/docker/otbr/docker-compose.yml`:

```
version: '3'
services:
  otbr:
    image: openthread/otbr:latest
    container_name: otbr
    network_mode: host
    privileged: true
    volumes:
      - /dev/ttyUSB0:/dev/ttyUSB0
\subsection{Despliegue de Servicios en Docker}
```

La plataforma del gateway se despliega mediante contenedores Docker orquestados con docker-compose. Los

```
\begin{itemize}
  \item \textbf{OpenThread Border Router (OTBR)}: Enrutamiento Thread/IPv6 (\texttt{/dev/ttyUSB0} → n)
  \item \textbf{ThingsBoard Edge}: Plataforma IoT local con sincronización Cloud
  \item \textbf{PostgreSQL + TimescaleDB}: Base de datos de series temporales
  \item \textbf{IEEE 2030.5 Server (SEP 2.0)}: API REST estándar para utilidades
  \item \textbf{Bridge ThreadTB}: Traductor MQTT entre redes Thread y ThingsBoard
  \item \textbf{Apache Kafka}: Bus de mensajes para integración empresarial
\end{itemize}
```

Los archivos `\texttt{docker-compose.yml}` completos para OTBR, ThingsBoard Edge, PostgreSQL y servicios a

El despliegue típico sigue esta secuencia:

```
\begin{verbatim}
cd /mnt/docker/otbr && docker-compose up -d
cd /mnt/docker/tb-edge && docker-compose up -d
cd /mnt/docker/sep20-server && docker-compose up -d
cd /mnt/docker/thread-bridge && docker-compose up -d
docker ps # Verificar todos los servicios activos

```

```
return Response(xml, mimetype='application/sep+xml')
```

```
@app.route('/tm', methods=['GET']) def timeSync() :"""
IEEE2030,5TimeSynchronization"""
import time
current_time = int(time.time())
xml = f"""<?xml version="1.0" encoding="UTF-8"?><Time xmlns="urn:ieee:std:2030.5:ns">
<currentTime>{current_time}</currentTime>
<quality>7</quality>
<!--0-->
<Time>{current_time}</Time>"""
return Response(xml, mimetype='application/sep+xml')
```

```
@app.route('/mup/<device_id>', methods=['GET']) def mirror_usage_point(device_id) :
"""
IEEE2030,5MeteringMirror"""
ConsultarTBEdge por el dispositivo
resp = requests.get(f"TBEDGEURL/{device_id}")
X-Authorization : "Bearer YOURTOKEN"
data = resp.json()
```

```
energy = data.get('energy_kwh', [])[0].get('value', 0)
timestamp = data.get('energy_kwh', [])[0].get('ts', 0) // 1000
```

```
xml = f"""<?xml version="1.0" encoding="UTF-8"?><MirrorUsagePoint xmlns="urn:ieee:std:2030.5:ns">
<mRID>{device_id}</mRID>
<MirrorMeterReading>
<Reading>
<value>{int(energy * 1000)}</value>
<start>{timestamp // 15}</start>
<duration>900</duration>
<start>{timestamp // 15}</start>
</timePeriod>
</Reading>
</MirrorMeterReading>
</MirrorUsagePoint>"""
return Response(xml, mimetype='application/sep+xml')
```

```
if name == 'main':
    app.run(host='0.0.0.0', port=8883, ssl_context=(server.crt, server.key))
```

Despliegue:

```
cd /mnt/docker/sep20-server
docker-compose up -d
docker logs -f sep20-server
```

Prueba de endpoint:

```
curl -k --cert client.crt --key client.key \
https://gateway:8883/dcap
```

## Configuración de Sincronización con Cloud

volumes: - ./tb-edge-data:/data - ./tb-edge-logs:/var/log/thingsboard depends<sub>on</sub>: -postgresrestart : unless-stopped

postgres: image: postgres:15-alpine container<sub>name</sub> : tb-edge-postgres environment : -POSTGRESDB = tb<sub>edge</sub>-POSTGRESUSER = postgres -POSTGRESPASSWORD = postgres123 volumes: -./postgres-data : /var/lib/postgresql/data restart : unless - stopped

Despliegue:

```
cd /mnt/docker/tb-edge
docker-compose up -d
docker logs -f tb-edge # Esperar inicio completo (~2 min)
```

Acceso web: <http://<gateway-ip>:8080> (credenciales por defecto: tenant@thingsboard.org / tenant)

## Configuración de Sincronización con Cloud

En ThingsBoard Cloud:

1. Crear Edge instance en *Edge Management*.
2. Copiar **Routing Key** y **Secret**.
3. Actualizar variables en `docker-compose.yml`.
4. Reiniciar contenedor: `docker-compose restart tb-edge`.

### 5.8.7 Integración OTBR ↔ ThingsBoard Edge

#### Flujo de Datos

1. Dispositivos Thread (nodos ESP32C6) publican datos vía CoAP/MQTT sobre Thread.
2. OTBR rutea tráfico IPv6 desde Thread a red LAN del gateway.
3. Aplicación bridge (Python/Node.js) suscrita a CoAP/MQTT convierte y publica a TB Edge vía MQTT.
4. TB Edge procesa localmente (reglas, alarmas) y sincroniza con cloud periódicamente.

## Script Bridge (Ejemplo Python)

Archivo /mnt/docker/bridge/bridge.py:

```
import paho.mqtt.client as mqtt
import json

# Cliente MQTT para recibir de dispositivos Thread
thread_client = mqtt.Client()
thread_client.connect("localhost", 1883)

# Cliente MQTT para publicar a TB Edge
tb_client = mqtt.Client()
tb_client.username_pw_set("ACCESS_TOKEN")
tb_client.connect("localhost", 1883)

def on_message(client, userdata, msg):
    # Parser de telemetría Thread
    data = json.loads(msg.payload)

    # Transformar a formato TB
    telemetry = {
        "ts": int(data["timestamp"]) * 1000,
        "values": [
            "energy": data["energy_kwh"],
            "power": data["power_w"],
            "voltage": data["voltage_v"]
        ]
    }

    # Publicar a TB Edge
    tb_client.publish("v1/devices/me/telemetry",
                      json.dumps(telemetry))

thread_client.on_message = on_message
thread_client.subscribe("thread/telemetry/#")
thread_client.loop_forever()
```

Desplegar como contenedor:

```
docker build -t thread-tb-bridge .
docker run -d --name bridge --network host thread-tb-bridge
```

## 5.9 Arquitectura de Datos: Kafka y PostgreSQL

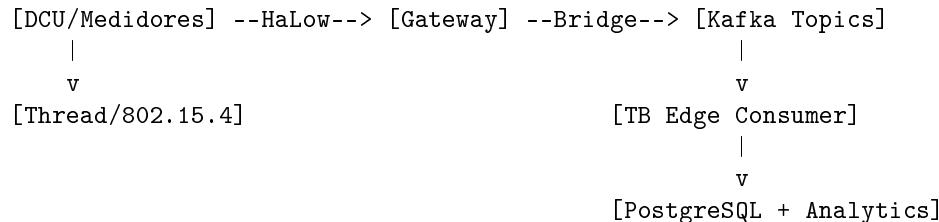
### 5.9.1 Integración de Apache Kafka

Apache Kafka proporciona una capa de mensajería distribuida de alto rendimiento para desacoplar productores (dispositivos IoT) de consumidores (ThingsBoard Edge, analítica, almacenamiento):

#### Rol de Kafka en la Arquitectura

- **Message broker:** Intermedia entre bridge (productor) y TB Edge (consumidor).
- **Buffer distribuido:** Almacena temporalmente mensajes en tópicos persistentes.
- **Escalabilidad:** Soporta >100k msg/s con múltiples particiones.
- **Durabilidad:** Retención configurable (7 días default) para replay histórico.

#### Arquitectura con Kafka:



#### Docker Compose para Kafka

Archivo /mnt/ssd/docker/kafka/docker-compose.yml:

```

version: '3.8'
services:
  zookeeper:
    image: confluentinc/cp-zookeeper:7.5.0
    container_name: zookeeper
    environment:
      ZOOKEEPER_CLIENT_PORT: 2181
      ZOOKEEPER_TICK_TIME: 2000
    volumes:
      - ./zookeeper-data:/var/lib/zookeeper/data
  
```

```

restart: unless-stopped

kafka:
  image: confluentinc/cp-kafka:7.5.0
  container_name: kafka
  depends_on:
    - zookeeper
  ports:
    - "9092:9092"
  environment:
    KAFKA_BROKER_ID: 1
    KAFKA_ZOOKEEPER_CONNECT: zookeeper:2181
    KAFKA_ADVERTISED_LISTENERS: PLAINTEXT://kafka:9092
    KAFKA_OFFSETS_TOPIC_REPLICATION_FACTOR: 1
    KAFKA_LOG_RETENTION_HOURS: 168 # 7 días
    KAFKA_LOG_SEGMENT_BYTES: 104857600 # 100 MB
    KAFKA_COMPRESSION_TYPE: gzip
  volumes:
    - ./kafka-data:/var/lib/kafka/data
  restart: unless-stopped

```

Crear tópicos:

```

docker exec -it kafka kafka-topics --create \
--bootstrap-server localhost:9092 \
--topic telemetry --partitions 3 --replication-factor 1

docker exec -it kafka kafka-topics --create \
--bootstrap-server localhost:9092 \
--topic alarms --partitions 2 --replication-factor 1

```

### Bridge Kafka Producer

Modificación del bridge para publicar a Kafka:

```

from kafka import KafkaProducer
import json

# Kafka producer
producer = KafkaProducer(
    bootstrap_servers=['localhost:9092'],
    value_serializer=lambda v: json.dumps(v).encode('utf-8'),
    compression_type='gzip'
)

def on_message(client, userdata, msg):
    data = json.loads(msg.payload)

```

```

# Publicar a Kafka topic 'telemetry'
producer.send('telemetry', {
    'device_id': data.get('device_id'),
    'timestamp': int(time.time() * 1000),
    'energy_kwh': data['energy_kwh'],
    'power_w': data['power_w'],
    'voltage_v': data['voltage_v']
})

# Flush cada 100 mensajes o 5 segundos
if msg_count % 100 == 0:
    producer.flush()

```

### TB Edge Kafka Consumer

ThingsBoard Edge configurado como consumidor Kafka:

```

# /mnt/ssd/docker/tb-edge-data/conf/tb-edge.yml
queue:
  type: kafka # Cambiar de 'in-memory' a 'kafka'
  kafka:
    bootstrap:
      servers: 'kafka:9092'
    topics:
      telemetry: 'telemetry'
      alarms: 'alarms'
    consumer:
      group_id: 'tb-edge-group'
      auto_offset_reset: 'earliest'
  producer:
    compression_type: 'gzip'
    acks: 1

```

### Ventajas de Kafka vs in-memory queue:

- **Capacidad:** GB de mensajes vs 100k en memoria.
- **Replay:** Consumir desde offset histórico para análisis.
- **Multi-consumidor:** TB Edge + analítica + ML simultáneamente.
- **Backpressure:** Kafka absorbe picos sin perder mensajes.

### 5.9.2 PostgreSQL: Base de Datos Persistente

#### Rol de PostgreSQL en la Arquitectura

PostgreSQL almacena:

- **Telemetría histórica:** Series temporales con extensión TimescaleDB.
- **Configuración de dispositivos:** Atributos, credenciales, relaciones.
- **Alarmas y eventos:** Log persistente para auditoría.
- **Dashboards y reglas:** Definiciones de Rule Engine TB Edge.

#### Optimización para Series Temporales (TimescaleDB)

TimescaleDB es una extensión de PostgreSQL optimizada para series temporales, que ofrece:

- **Compresión:** 10-20× reducción en espacio disco mediante algoritmos adaptativos
- **Queries rápidas:** Particionamiento automático por tiempo (chunks de 7 días por defecto)
- **Agregaciones:** Función `time_bucket` para promedios 15-min/1-hora con vistas materializadas
- **Retención automática:** Elimina datos antiguos sin intervención manual

El esquema completo de TimescaleDB, incluyendo la definición de hypertables, políticas de compresión, continuous aggregates (vistas materializadas para agregaciones de 15-min, 1-hora y 1-día), políticas de retención (90 días), y cinco consultas SQL de ejemplo (telemetría reciente, consumo diario, alertas de voltaje, promedios semanales y agregados de facturación mensual), se presenta en el Anexo D. El docker-compose de TimescaleDB se documenta en el Anexo B.

Ejemplo de consulta para consumo promedio por hora:

```
SELECT
    device_id,
    time_bucket('1 hour', time) AS hour,
    AVG(energy_kwh) AS avg_energy,
    MAX(power_w) AS peak_power
FROM telemetry
WHERE time > NOW() - INTERVAL '24 hours'
GROUP BY device_id, hour
ORDER BY device_id, hour DESC;
```

## 5.10 Protocolos de Comunicación IoT

### 5.10.1 Comparación de Protocolos

Característica	MQTT	CoAP	HTTP/REST	LwM2M
Capa OSI	Aplicación	Aplicación	Aplicación	Aplicación
Transporte	TCP	UDP	TCP	UDP (CoAP)
Overhead	2 bytes	4 bytes	>100 bytes	4-20 bytes
QoS niveles	0, 1, 2	CON, NON, ACK	N/A	CON, NON
Pub/Sub	Sí	No	No	No
Observación	No	Sí (Observe)	No	Sí (Observe)
Device Mgmt	No	No	No	Sí (objetos)
Seguridad	TLS/mTLS	DTLS	TLS/mTLS	DTLS + PSK
Payload	Binario/JSON	CBOR/JSON	JSON/XML	CBOR/TLV
Uso típico	Telemetría	Sensores low-power	APIs web	Device mgmt

Tabla 5-5: Comparación de protocolos IoT

### 5.10.2 MQTT (Message Queuing Telemetry Transport)

#### Características MQTT

- **Patrón Pub/Sub:** Desacoplamiento productor/consumidor vía broker.
- **QoS 0 (At most once):** Sin confirmación, mínima latencia.
- **QoS 1 (At least once):** Con ACK, puede duplicar mensajes.
- **QoS 2 (Exactly once):** Handshake 4-way, sin duplicados.
- **Retained messages:** Último valor almacenado en broker para nuevos suscriptores.
- **Last Will Testament (LWT):** Notificación automática de desconexión.

#### Uso en Gateway

##### Topics utilizados:

```
# Telemetría uplink (dispositivo → TB Edge)
v1/devices/me/telemetry          # Formato ThingsBoard
smartgrid/meter/{id}/energy      # Formato personalizado
thread/telemetry/{node_id}       # Desde OTBR

# Comandos downlink (TB Edge → dispositivo)
v1/devices/me/rpc/request/{requestId}
```

```
smartgrid/meter/{id}/command

# LWT (detectar desconexión)
smartgrid/meter/{id}/status      # "online"/"offline"
```

#### Configuración broker Mosquitto en gateway:

```
# /etc/mosquitto/mosquitto.conf
listener 1883          # Puerto MQTT
listener 8883          # Puerto MQTTS (TLS)
cafile /etc/mosquitto/ca.crt
certfile /etc/mosquitto/server.crt
keyfile /etc/mosquitto/server.key
require_certificate true

# Persistencia
persistence true
persistence_location /mnt/ssd/mosquitto/

# Autenticación
allow_anonymous false
password_file /etc/mosquitto/passwd

# QoS máximo
max_qos 2

# Retención de mensajes
max_queued_messages 1000
message_size_limit 8192
```

### 5.10.3 CoAP (Constrained Application Protocol)

#### Características CoAP

- **Protocolo UDP:** Menor overhead que TCP (4 bytes header vs 20 bytes).
- **RESTful:** Métodos GET /POST /PUT /DELETE como HTTP.
- **Observe:** Cliente se suscribe a recurso, servidor notifica cambios.
- **Block-wise transfer:** Fragmentación para mensajes >1024 bytes.
- **DTLS:** Seguridad con Pre-Shared Keys (PSK) o certificados.

## Uso en Thread/OpenThread

OpenThread usa CoAP nativamente para comunicación mesh:

```
# Recurso CoAP en nodo Thread
coap://[fd00::1234:5678:abcd]/meter/energy

# GET request (cliente OTBR)
coap-client -m GET coap://[fd00::1234:5678:abcd]/meter/energy
# Response: {"energy_kwh": 100.5, "power_w": 1200}

# POST command (enviar comando)
coap-client -m POST coap://[fd00::1234:5678:abcd]/config/interval \
-e '{"interval_sec": 300}'

# Observe (suscripción a cambios)
coap-client -m GET -s 60 coap://[fd00::1234:5678:abcd]/meter/energy
# Server notifica cada vez que cambia el valor
```

## Bridge CoAP → MQTT:

```
import asyncio
from aiocoap import *

async def coap_to_mqtt_bridge():
    protocol = await Context.create_client_context()

    # Observe CoAP resource
    request = Message(code=GET,
                      uri='coap://[fd00::1234]/meter/energy',
                      observe=0)

    async for response in protocol.request(request).observation:
        # Parse CoAP payload
        data = json.loads(response.payload)

        # Publish to MQTT
        mqtt_client.publish('thread/telemetry/1234',
                            json.dumps(data))
```

### 5.10.4 HTTP/REST

#### Uso en Gateway

HTTP/REST se usa para:

- **APIs de gestión:** TB Edge API, IEEE 2030.5 Server.
- **Integraciones externas:** Webhooks, consultas a cloud.
- **Configuración:** LuCI web UI, Ollama API.

#### Ejemplos de APIs:

```
# ThingsBoard Edge API
GET http://gateway:8080/api/tenant/devices
Authorization: Bearer {token}

# IEEE 2030.5 REST API
GET https://gateway:8883/dcap
Client-Cert: meter-001.crt

# Ollama LLM API
POST http://gateway:11434/api/generate
Content-Type: application/json
{"model": "llama3.2:3b", "prompt": "Analiza consumo..."}

# LuCI configuration
POST http://gateway/cgi-bin/luci/admin/network/wireless
```

### 5.10.5 LwM2M (Lightweight M2M)

#### Características LwM2M

- **Gestión de dispositivos:** Bootstrap, configuración remota, firmware OTA
- **Modelo de objetos:** Jerarquía Object/Instance/Resource (ej. Device/0/Manufacturer)
- **Operaciones:** Read, Write, Execute, Observe, Discover
- **Transporte:** CoAP sobre UDP (binding U) o SMS/NB-IoT (binding S)

## Objetos LwM2M Estándar (OMA SpecWorks)

Los objetos LwM2M utilizados incluyen:

- **Objeto 0 (Security)**: Server URI, PSK, Bootstrap
- **Objeto 1 (Server)**: Lifetime, Binding, Registration
- **Objeto 3 (Device)**: Manufacturer, Model, Serial Number, Battery, Memory, Reboot
- **Objeto 4 (Connectivity)**: Network Bearer, IP Address, Signal Strength
- **Objeto 5 (Firmware Update)**: Package URI, Update State, Execute Update
- **Objeto 6 (Location)**: Latitude, Longitude, Timestamp
- **Objeto 3303 (Temperature)**: Sensor Value, Units, Min/Max, Reset
- **Objeto 3304 (Humidity)**: Sensor Value, Units, Min/Max
- **Objeto 3312 (On/Off)**: Digital Output State (boolean)

La implementación completa de referencia de un nodo IoT ESP32-C6 con cliente LwM2M AVSystems Anjay, incluyendo todos los archivos de código fuente (`main.c`, `lwm2m_client.c`, `temp_object.c`, `humidity_object.c`, `device_object.c`, `connectivity_object.c`, `location_object.c`, `onoff_object.c`, `thread_prov.c`), el `CMakeLists.txt`, instrucciones de compilación con ESP-IDF, y comandos de comisionamiento Thread/LwM2M, se documenta en el Anexo E.

## Ventajas LwM2M para Smart Metering

- **Estandarización**: Objetos interoperables (OMA SpecWorks)
- **Gestión centralizada**: Bootstrap, firmware OTA desde gateway
- **Eficiencia**: DTLS+PSK consume menos que TLS+X.509 (clave de 16 bytes vs certificado 2 KB)
- **Observe**: Notificaciones automáticas sin polling (ahorro energético)

### 5.10.6 Selección de Protocolo por Caso de Uso

## 5.11 Resiliencia y Almacenamiento Persistente (SSD)

### 5.11.1 Arquitectura de Almacenamiento del Gateway

El gateway implementa una estrategia de almacenamiento de alta resiliencia:

Caso de Uso	Protocolo	Justificación
Telemetría medidor → Gateway	MQTT QoS 1	Pub/Sub, QoS garantizado, broker local
Thread mesh intra-nodo	CoAP	UDP eficiente, Observe nativo
Gateway → TB Cloud	MQTT QoS 1 / HTTP	TLS seguro, compresión gzip
Device management (FW OTA)	LwM2M	Objetos estándar, bootstrap
APIs configuración gateway	HTTP/REST	LuCI, TB Edge API
IEEE 2030.5 Smart Energy	HTTP/REST	Estándar mandatorio (SEP 2.0)
Comandos downlink (RPC)	MQTT QoS 1	Baja latencia, ACK confirmado
Alarmas críticas	MQTT QoS 2	Exactly-once, sin duplicados

Tabla 5-6: Selección de protocolo por caso de uso

- **Flash interna (128 MB):** Sistema operativo OpenWRT y configuración UCI.
- **SSD M.2 NVMe (256 GB):** Datos persistentes Docker, PostgreSQL, cola ThingsBoard Edge.
- **USB 3.0 (opcional):** Backups periódicos y recuperación de desastres.

#### Ventajas SSD NVMe vs USB/SD:

- **Durabilidad:** >1M ciclos E/W (vs 10k-100k en SD), MTBF >1.5M horas.
- **Desempeño:** >3000 IOPS escritura (vs <100 IOPS USB 2.0), latencia <0.1ms.
- **Fiabilidad:** ECC interno, power-loss protection (PLP), SMART monitoring.

Montaje automático SSD en /mnt/ssd:

```
# /etc/config/fstab
config mount
    option device '/dev/nvme0n1p1'
    option target '/mnt/ssd'
    option fstype 'ext4'
    option options 'rw,relatime,noatime'
    option enabled '1'
    option enabled_fsck '1'
```

Estructura de directorios:

```
/mnt/ssd/
docker/          # Volúmenes Docker
tb-edge-data/    # Configuración TB Edge
postgres-data/   # Base de datos PostgreSQL
queue/           # Cola de mensajes offline
otbr-config/     # Configuración Thread
bridge-logs/     # Logs del bridge
backups/          # Backups automáticos
tmp/              # Directorio temporal (tmpfs en RAM)
```

### 5.11.2 ThingsBoard Edge Queue: Resiliencia Offline

#### Arquitectura de Cola Persistente

ThingsBoard Edge implementa una **cola de mensajes persistente** para garantizar resiliencia ante pérdida de conectividad cloud:

- **Queue storage:** PostgreSQL + filesystem (/mnt/ssd/docker/queue).
- **Capacidad:** Hasta 100k mensajes en cola (configurable, 500 MB con CBOR).
- **Política FIFO:** Mensajes más antiguos se sincronizan primero al recuperar conectividad.
- **Priorización:** Alarmas críticas tienen mayor prioridad que telemetría histórica.

#### Configuración de Queue en TB Edge

Archivo /mnt/ssd/docker/tb-edge-data/conf/tb-edge.yml:

```

queue:
  type: in-memory # 0 'kafka' para mayor capacidad
  in_memory:
    max_elements: 100000
    max_size_bytes: 524288000 # 500 MB

cloud_sync:
  # Intervalo de sincronización con cloud
  sync_interval: 300 # 5 minutos (online)
  offline_sync_interval: 3600 # 1 hora (detectado offline, reintentos)

  # Batch size para sincronización
  batch_size: 1000 # Mensajes por batch
  max_batch_size: 5000 # Máximo en condiciones de catch-up

  # Compresión de datos
  compression_enabled: true
  compression_type: gzip # 0 'lz4' para menor CPU

  # Retry policy
  max_retries: 10
  retry_interval: 60 # segundos entre reintentos
  backoff_multiplier: 2 # Exponential backoff

persistent_queue:
  path: /data/queue
  max_disk_usage_mb: 2000 # 2 GB límite en disco

```

```
write_batch_size: 100
flush_interval_ms: 1000
```

## Flujo de Operación con Queue

### Modo Online (conectividad cloud activa):

1. TB Edge recibe telemetría de dispositivos vía MQTT (puerto 1883).
2. Procesa reglas locales (alarmas, transformaciones).
3. Encola mensaje en queue in-memory.
4. Cada 5 minutos, sincroniza batch de 1000 mensajes con TB Cloud vía gRPC (puerto 7070).
5. Al confirmar ACK del cloud, elimina mensajes de la cola.

### Modo Offline (sin conectividad cloud):

1. TB Edge detecta pérdida de conexión (timeout gRPC >30s).
2. Cambia a modo offline: continúa procesamiento local.
3. Mensajes se acumulan en queue persistente (PostgreSQL + filesystem).
4. Dashboards locales permanecen funcionales (<http://<gateway-ip>:8080>).
5. Alarmas se ejecutan localmente (email, webhook a sistemas locales).
6. Queue crece hasta límite configurado (100k msgs o 2 GB).

### Recuperación de Conectividad (catch-up sync):

1. TB Edge detecta reconexión con cloud (gRPC handshake exitoso).
2. Inicia sincronización acelerada: batch size aumenta a 5000 mensajes.
3. Prioriza alarmas/eventos críticos (priority queue).
4. Comprime datos con gzip (40-60 % reducción).
5. Sincroniza backlog completo en 10-15 minutos (100k msgs @ 5000/batch).
6. Al terminar, retorna a modo online normal (batch 1000, intervalo 5 min).

## Protección contra Desbordamiento de Queue

Política de gestión de capacidad:

```
# /mnt/ssd/docker/tb-edge-data/scripts/queue-monitor.sh
#!/bin/sh

QUEUE_SIZE=$(du -sm /mnt/ssd/docker/queue | cut -f1)
MAX_SIZE=1800 # 1.8 GB (90% del límite de 2 GB)

if [ $QUEUE_SIZE -gt $MAX_SIZE ]; then
    logger -t TB-EDGE "Queue size critical: ${QUEUE_SIZE}MB"

    # Estrategia 1: Eliminar telemetría histórica (>7 días)
    find /mnt/ssd/docker/queue -name "*.telemetry" \
        -mtime +7 -delete

    # Estrategia 2: Comprimir eventos no críticos
    find /mnt/ssd/docker/queue -name "*.event" \
        -mtime +1 -exec gzip {} \;

    # Estrategia 3: Notificar operador
    curl -X POST http://localhost:8080/api/v1/telemetry \
        -d '{"queue_overflow":true,"size_mb":'$QUEUE_SIZE'}'
fi
```

Ejecutar vía cron cada hora:

```
# crontab -e
0 * * * * /mnt/ssd/docker/tb-edge-data/scripts/queue-monitor.sh
```

### 5.11.3 Resiliencia Multinivel

Nivel	Componente	Mecanismo de Resiliencia	RTO
L1 Hardware	SSD NVMe	ECC, PLP, SMART monitoring	0s
L2 Filesystem	ext4	Journaling, fsck automático	<30s
L3 Base de datos	PostgreSQL	WAL, autovacuum, replication slots	<60s
L4 Aplicación	TB Edge Queue	Persistent queue, retry policy, compression	<300s
L5 Red	mwlan3	WAN failover Ethernet/LTE, tracking activo	<30s
L6 Container	Docker + Watchtower	Healthchecks, restart policy, auto-updates	<120s

Tabla 5-7: Niveles de resiliencia en gateway con RTO (Recovery Time Objective)

## 5.12 Gestión Remota del Gateway

### 5.12.1 Feeds de OpenWRT

#### Arquitectura de Feeds

OpenWRT utiliza **feeds** (repositorios de paquetes) para extender funcionalidad del sistema base:

- **Feed base:** Paquetes esenciales incluidos en imagen oficial.
- **Feed packages:** Paquetes comunitarios adicionales (>10k paquetes).
- **Feed luci:** Interfaz web LuCI y aplicaciones.
- **Feed routing:** Protocolos de routing avanzados (batman-adv, olsr).
- **Feed telephony:** VoIP y telefonía.
- **Feeds custom:** Repositorios personalizados (enterprise, vendor-specific).

#### Configuración de Feeds

Archivo /etc/opkg/distfeeds.conf:

```
# Feeds oficiales OpenWRT 23.05
src/gz openwrt_core https://downloads.openwrt.org/releases/23.05.0/targets/ramips/mt7621/packages
src/gz openwrt_base https://downloads.openwrt.org/releases/23.05.0/packages/mipsel_24kc/base
src/gz openwrt_luci https://downloads.openwrt.org/releases/23.05.0/packages/mipsel_24kc/luci
src/gz openwrt_packages https://downloads.openwrt.org/releases/23.05.0/packages/mipsel_24kc/packages
src/gz openwrt_routing https://downloads.openwrt.org/releases/23.05.0/packages/mipsel_24kc/routing

# Feed personalizado para Smart Grid (interno empresa)
src/gz smartgrid_custom https://repo.empresa.com/openwrt/23.05/smartgrid
option check_signature 1
```

#### Gestión de Paquetes con opkg

##### Comandos esenciales:

```
# Actualizar lista de paquetes desde feeds
```

```

opkg update

# Buscar paquetes
opkg find "*halow*"
opkg find "*docker*"

# Instalar paquete
opkg install luci-app-dockerman
opkg install mwan3 luci-app-mwan3

# Listar paquetes instalados
opkg list-installed | grep docker

# Actualizar paquete específico
opkg upgrade docker

# Actualizar todos los paquetes
opkg list-upgradable
opkg upgrade $(opkg list-upgradable | awk '{print $1}')

# Remover paquete (mantener configuración)
opkg remove --force-removal-of-dependent-packages docker

# Información de paquete
opkg info docker

```

## Feed Custom para Smart Grid

Crear feed interno con paquetes personalizados:

### Estructura del feed:

```

smartgrid-feed/
|-- Makefile
|-- packages/
|   |-- halow-driver-morse/
|   |   |-- Makefile
|   |   +-- files/
|   |-- tb-edge-connector/
|   |   |-- Makefile
|   |   +-- src/
|   |-- ieee2030-server/
|   |   |-- Makefile
|   |   +-- files/
+-- mcp-l1m-client/
    |-- Makefile
    +-- src/
--- README.md

```

**Ejemplo Makefile para paquete personalizado:**

```
# packages/tb-edge-connector/Makefile
include $(TOPDIR)/rules.mk

PKG_NAME:=tb-edge-connector
PKG_VERSION:=1.0.0
PKG_RELEASE:=1

include $(INCLUDE_DIR)/package.mk

define Package/tb-edge-connector
SECTION:=smartgrid
CATEGORY:=SmartGrid
TITLE:=ThingsBoard Edge Connector
DEPENDS:+=python3 +python3-paho-mqtt +python3-requests
endef

define Package/tb-edge-connector/description
Connector para integrar dispositivos Thread con TB Edge
endef

define Build/Compile
# Script Python, no requiere compilación
endef

define Package/tb-edge-connector/install
$(INSTALL_DIR) $(1)/usr/bin
$(INSTALL_BIN) ./src/tb_connector.py $(1)/usr/bin/
$(INSTALL_DIR) $(1)/etc/config
$(INSTALL_CONF) ./files/tb-connector.conf $(1)/etc/config/
$(INSTALL_DIR) $(1)/etc/init.d
$(INSTALL_BIN) ./files/tb-connector.init $(1)/etc/init.d/tb-connector
endef

$(eval $(call BuildPackage,tb-edge-connector))
```

**Hosting del feed:**

```
# Generar índice de paquetes
cd smartgrid-feed
make package/index

# Servir vía HTTP (nginx)
server {
    listen 80;
    server_name repo.empresa.com;
    root /var/www/openwrt-feed;

    location /openwrt/23.05/smartgrid {
```

```

        autoindex on;
    }
}

```

### 5.12.2 OpenVPN: Acceso Remoto Seguro

#### Rol de OpenVPN en la Arquitectura

OpenVPN proporciona túnel VPN cifrado para gestión remota del gateway:

- **Acceso SSH:** Administración CLI segura desde NOC (Network Operations Center).
- **LuCI web UI:** Acceso a interfaz de configuración sin exponer puerto 80/443 a internet.
- **Debugging:** Logs remotos, captura de tráfico (tcpdump), análisis de performance.
- **Túnel permanente:** Gateway se conecta automáticamente a servidor VPN central (hub-spoke).

#### Instalación OpenVPN en Gateway

```

opkg update
opkg install openvpn-openssl luci-app-openvpn

```

#### Configuración Cliente OpenVPN

Archivo /etc/openvpn/client.conf:

```

client
dev tun0
proto udp
remote vpn.empresia.com 1194

# Certificados PKI
ca /etc/openvpn/ca.crt
cert /etc/openvpn/gateway-001.crt
key /etc/openvpn/gateway-001.key
tls-auth /etc/openvpn/ta.key 1

# Compresión
comp-lzo adaptive

```

```
# Keepalive (detectar desconexión en 120s)
keepalive 10 120

# Persistencia de túnel
persist-key
persist-tun

# Logging
verb 3
log-append /var/log/openvpn.log

# Pull routes desde servidor (acceso a red NOC)
pull

# Reconexión automática
resolv-retry infinite
nobind

# Usuario sin privilegios (seguridad)
user nobody
group nogroup
```

**Configuración UCI (OpenWRT native):**

```
# /etc/config/openvpn
config openvpn 'noc_tunnel'
    option enabled '1'
    option client '1'
    option dev 'tun0'
    option proto 'udp'
    option remote 'vpn.empresa.com 1194'
    option ca '/etc/openvpn/ca.crt'
    option cert '/etc/openvpn/gateway-001.crt'
    option key '/etc/openvpn/gateway-001.key'
    option tls_auth '/etc/openvpn/ta.key 1'
    option comp_lzo 'adaptive'
    option keepalive '10 120'
    option persist_key '1'
    option persist_tun '1'
    option verb '3'
```

**Iniciar servicio:**

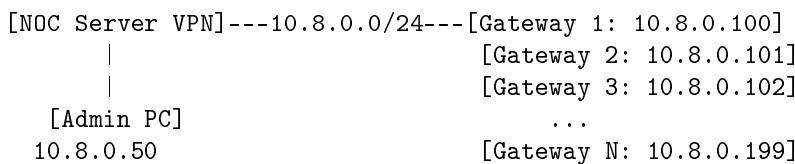
```
/etc/init.d/openvpn enable
/etc/init.d/openvpn start

# Verificar túnel
ifconfig tun0
# Esperado: inet addr:10.8.0.100
```

```
ping 10.8.0.1 # Servidor VPN
```

### Servidor OpenVPN Central (NOC)

Arquitectura hub-spoke:



Configuración servidor (/etc/openvpn/server.conf):

```
port 1194
proto udp
dev tun
server 10.8.0.0 255.255.255.0

# Certificados
ca ca.crt
cert server.crt
key server.key
dh dh2048.pem
tls-auth ta.key 0

# Client-to-client (permitir gateways comunicarse entre sí)
client-to-client

# Push routes a clientes (red NOC)
push "route 10.10.0.0 255.255.255.0"

# Persistencia
keepalive 10 120
persist-key
persist-tun

# Logging
status /var/log/openvpn-status.log
log-append /var/log/openvpn.log
verb 3

# Client config dir (configuración por cliente)
client-config-dir /etc/openvpn/ccd

# Compresión
```

---

```
comp-lzo adaptive
```

#### Configuración específica por gateway (CCD):

```
# /etc/openvpn/ccd/gateway-001
# Asignar IP fija 10.8.0.100
ifconfig-push 10.8.0.100 10.8.0.101

# Push ruta específica para este gateway (red Thread local)
push "route 192.168.50.0 255.255.255.0"
```

### 5.12.3 OpenWISP: Gestión Centralizada de Gateways

#### Arquitectura OpenWISP

OpenWISP es una plataforma open-source para gestión masiva de dispositivos OpenWRT:

- **OpenWISP Controller:** Backend Django para gestión de configuraciones.
- **OpenWISP Config:** Agente en gateway que aplica configuraciones remotas.
- **OpenWISP Monitoring:** Colección de métricas (CPU, RAM, tráfico).
- **OpenWISP Firmware Upgrader:** Actualizaciones OTA masivas.
- **OpenWISP Network Topology:** Visualización de topología de red.

#### Componentes:

```
[OpenWISP Server]---HTTPS/VPN---[Gateway Fleet (100-1000 gateways)]
|                               |
|--- Controller (Django)      |--- openwisp-config (agente)
|--- PostgreSQL                |--- openwisp-monitoring
|--- Redis                     +--- Actualizacion UCI automatica
|--- Celery
+--- Web Dashboard
```

#### Instalación OpenWISP Config en Gateway

```
opkg update
```

```
opkg install openwisp-config openwisp-monitoring
```

```
# Configurar agente
uci set openwisp.http.url='https://controller.empresa.com'
uci set openwisp.http.shared_secret='YOUR_SHARED_SECRET'
uci set openwisp.http.consistent_key='GATEWAY_UUID'
uci set openwisp.http.verify_ssl='1'
uci commit openwisp

# Habilitar servicios
/etc/init.d/openwisp_config enable
/etc/init.d/openwisp_monitoring enable
/etc/init.d/openwisp_config start
/etc/init.d/openwisp_monitoring start
```

## Despliegue OpenWISP Controller (Docker)

```
# docker-compose.yml para OpenWISP Server
version: '3.8'
services:
  postgres:
    image: postgres:15
    environment:
      POSTGRES_DB: openwisp_db
      POSTGRES_USER: openwisp
      POSTGRES_PASSWORD: changeme
    volumes:
      - postgres-data:/var/lib/postgresql/data

  redis:
    image: redis:7-alpine

  openwisp-dashboard:
    image: openwisp/openwisp-dashboard:latest
    depends_on:
      - postgres
      - redis
    ports:
      - "443:443"
    environment:
      DB_ENGINE: django.db.backends.postgresql
      DB_NAME: openwisp_db
      DB_USER: openwisp
      DB_PASSWORD: changeme
      DB_HOST: postgres
      REDIS_HOST: redis
      DJANGO_SECRET_KEY: changeme
      DJANGO_ALLOWED_HOSTS: controller.empresa.com
    volumes:
      - openwisp-media:/opt/openwisp/media
      - openwisp-static:/opt/openwisp/static
```

```

celery:
  image: openwisp/openwisp-dashboard:latest
  depends_on:
    - postgres
    - redis
  command: celery -A openwisp worker -l info
environment:
  DB_ENGINE: django.db.backends.postgresql
  DB_NAME: openwisp_db
  DB_USER: openwisp
  DB_PASSWORD: changeme
  DB_HOST: postgres
  REDIS_HOST: redis

```

## Gestión de Configuraciones

### Template UCI en OpenWISP Controller:

```

# Template "Smart Grid Gateway Base Config"
# network.json
{
  "network": [
    {
      "interface": "wan_eth",
      "proto": "dhcp",
      "metric": "10"
    },
    {
      "interface": "wan_lte",
      "proto": "modemmanager",
      "device": "/dev/ttyUSB2",
      "apn": "{{apn}}",
      "metric": "20"
    },
    {
      "interface": "halow",
      "proto": "static",
      "ipaddr": "{{halow_ip}}",
      "netmask": "255.255.255.0"
    }
  ],
  "wireless": [
    {
      "radio": "halow",
      "channel": "{{halow_channel}}",
      "mode": "ap",
      "ssid": "SmartGrid-{{site_id}}",
      "encryption": "sae",
      "key": "{{halow_password}}"
    }
  ]
}

```

```

    }
]
}
}
```

**Aplicar configuración desde dashboard:**

1. Crear template con variables ({{apn}}, {{halow\_channel}}).
2. Asignar template a grupo de gateways (ej. "Zona Norte - 50 gateways").
3. Definir variables por gateway o grupo.
4. Push configuración: OpenWISP genera UCI y envía a gateways vía HTTPS.
5. Agente openwisp-config aplica cambios: `uci commit && reload_config`.

**Firmware Upgrader: Actualización OTA Masiva****Workflow de actualización:**

1. Subir nueva imagen OpenWRT a OpenWISP Controller.
2. Crear **build** con imagen y checksum SHA256.
3. Asignar build a grupo de gateways (ej. "Firmware 23.05.2 - Gateways Zona Sur").
4. Programar actualización: inmediata o ventana de mantenimiento (3 AM).
5. OpenWISP envía comando a gateways.
6. Gateway descarga imagen vía HTTPS, verifica checksum, instala (sysupgrade), reinicia.
7. Gateway reporta versión actualizada post-reboot.

**Actualización segura (dual-partition):**

- **Partition A:** Firmware actual (activo).
- **Partition B:** Nueva imagen descargada.
- Escribir en Partition B, reiniciar, bootloader cambia a B.
- Si falla (no boot en 3 reintentos), rollback automático a Partition A.

## Monitoring y Alertas

OpenWISP Monitoring recolecta métricas:

- **Uptime:** Tiempo desde último reinicio.
- **CPU/RAM:** Load average, memoria disponible.
- **Storage:** Uso de SSD NVMe (`df -h /mnt/ssd`).
- **Interfaces:** Tráfico RX/TX, errores, señal HaLow/LTE.
- **Conectividad:** Ping a gateway (heartbeat), VPN status.
- **Docker:** Containers running/stopped, CPU/RAM por container.

Configuración alertas:

```
# OpenWISP Controller > Alerts
Alert: Gateway Offline
  Condition: ping_failed > 5 min
  Action: Email admin@empresa.com, SMS +57300...
Alert: High CPU Usage
  Condition: cpu_load_1min > 3.0 for 10 min
  Action: Email ops@empresa.com, Log to Syslog
Alert: Low Disk Space
  Condition: disk_usage_percent > 85%
  Action: Email admin@empresa.com, Trigger cleanup script
Alert: LTE Failover Active
  Condition: wan_interface = "wwan0" for 30 min
  Action: Email ops@empresa.com (posible fallo fibra)
```

### 5.12.4 Comparación de Herramientas de Gestión

Recomendación para despliegue Smart Grid:

- **Piloto (<10 gateways):** LuCI + OpenVPN + SSH.
- **Producción (10-100 gateways):** OpenVPN + OpenWISP.
- **Escala (>100 gateways):** OpenWISP completo + dual-partition firmware + VPN permanente.

Característica	LuCI (local)	OpenVPN + SSH	OpenWISP
Gestión masiva	No	No (manual)	Sí (100-1000 GWs)
Configuración remota	Manual (web UI)	CLI manual	Automática (templates)
Firmware OTA	Manual (sysupgrade)	SCP + sysupgrade	Automático (schedule)
Monitoreo	No (stats básicas)	Manual (SSH logs)	Automático (dashboard)
Alertas	No	No	Sí (email/SMS/webhook)
Rollback	Manual	Manual	Automático (dual-part)
Zero-touch provisioning	No	No	Sí (bootstrap)
Escalabilidad	1 gateway	<10 gateways	100-10,000 gateways
Costo	\$0	\$0	\$0 (open-source)

Tabla 5-8: Comparación de herramientas de gestión para gateway OpenWRT

## 5.13 Gestión de Uplink Redundante (Ethernet + LTE)

### 5.13.1 Política de Failover Automático

OpenWRT implementa failover basado en métricas de ruta (route metrics):

```
# /etc/config/network
config interface 'wan_eth'
    option proto 'dhcp'
    option ifname 'eth0.2'
    option metric '10' # Prioridad alta (menor = mejor)

config interface 'wan_lte'
    option proto 'modemmanager'
    option device '/sys/devices/.../usb1/1-1'
    option apn 'internet.movistar.com.co'
    option metric '20' # Prioridad baja (backup)
```

#### Comportamiento:

1. Kernel selecciona ruta con menor métrica (Ethernet, metric=10).
2. Si Ethernet falla (link down), kernel cambia automáticamente a LTE (metric=20).
3. Al recuperar Ethernet, kernel restaura la ruta principal.
4. Tiempo de comutación: <30 segundos (incluyendo renegociación TCP).

### 5.13.2 Monitoreo Activo de Conectividad (mwan3)

Paquete `mwan3` proporciona tracking proactivo de enlaces WAN:

```

opkg install mwan3 luci-app-mwan3

# /etc/config/mwan3
config interface 'wan_eth'
    option enabled '1'
    option track_ip '8.8.8.8 1.1.1.1'
    option track_method 'ping'
    option reliability '2' # Fallar tras 2 pings perdidos
    option count '3'
    option timeout '2'
    option interval '5'

config interface 'wan_lte'
    option enabled '1'
    option track_ip '8.8.4.4'
    option reliability '1'

config policy 'balanced'
    list use_member 'wan_eth_m1_w3' # 75% tráfico por Ethernet
    list use_member 'wan_lte_m1_w1' # 25% tráfico por LTE

config rule 'mqtt_prioritize_eth'
    option dest_port '8883'
    option proto 'tcp'
    option use_policy 'wan_eth_only' # MQTT solo por Ethernet

```

Verificación de estado:

```

mwan3 status # Estado de interfaces y tracking
mwan3 interfaces # Latencia y pérdida de paquetes por WAN

```

### 5.13.3 Optimización de Costos LTE

Estrategias para minimizar consumo de datos celulares:

#### Compresión de Datos

- **CBOR vs JSON:** Reducción de 40-60 % en tamaño de payload.

```

# JSON: 150 bytes
{"ts":1730000000000,"values":{"energy_kwh":1234.56,...}}

# CBOR: 85 bytes (43% reducción)
A2 63 746D70 1B... (formato binario compacto)

```

- **Batching:** TB Edge acumula 5 minutos de telemetría y envía en un solo paquete HTTP/2.
- **Compresión gzip:** Activar en cliente MQTT para payloads >1 KB.

## Políticas de Tráfico por WAN

Script de hotplug para adaptar comportamiento según WAN activa:

```
# /etc/hotplug.d/iface/99-wan-monitor
#!/bin/sh

if [ "$INTERFACE" = "wan_lte" ] && [ "$ACTION" = "ifup" ]; then
    logger "LTE activo - modo ahorro de datos"
    # Detener actualizaciones Docker
    killall -STOP watctower
    # Aumentar intervalo de sincronización TB Edge (1h en lugar de 5 min)
    docker exec tb-edge sh -c \
        "sed -i 's/CLOUD_SYNC_INTERVAL=300/CLOUD_SYNC_INTERVAL=3600/' /data/conf/thingsboard.yml"
    docker restart tb-edge
fi

if [ "$INTERFACE" = "wan_eth" ] && [ "$ACTION" = "ifup" ]; then
    logger "Ethernet recuperado - modo normal"
    killall -CONT watctower
    docker exec tb-edge sh -c \
        "sed -i 's/CLOUD_SYNC_INTERVAL=3600/CLOUD_SYNC_INTERVAL=300/' /data/conf/thingsboard.yml"
    docker restart tb-edge
fi
```

## Monitoreo de Consumo de Datos

```
# Instalar vnstat para estadísticas de tráfico
opkg install vnstat

# Inicializar base de datos para interfaz LTE
vnstat -u -i wwan0

# Consultar consumo mensual
vnstat -m -i wwan0
# Salida:
#   wwan0 / monthly
#   month      rx      |      tx      |      total
#   -----+-----+-----+
#   2025-10    2.5 GiB |    1.2 GiB |    3.7 GiB
```

Configurar alarma si consumo >10 GB/mes:

```
# /etc/crontabs/root
0 0 * * * /usr/bin/check-lte-quota.sh

# /usr/bin/check-lte-quota.sh
#!/bin/sh
USAGE=$(vnstat -m -i wwan0 | awk '/2025-10/{print $4}' | sed 's/GiB//')
if [ $(echo "$USAGE > 10" | bc) -eq 1 ]; then
    logger -t LTE "Cuota excedida: ${USAGE} GB - desabilitando LTE"
    ifdown wan_lte
    # Enviar alerta a TB Edge
    curl -X POST http://localhost:8080/api/v1/telemetry \
        -d '{"lte_quota_exceeded":true,"usage_gb":"'${USAGE}'"}'
fi
```

## 5.14 Gestión y Monitoreo del Gateway

### 5.14.1 Interfaz de Gestión (LuCI)

OpenWRT proporciona interfaz web LuCI en `http://<gateway-ip>:80`:

- **Network:** Configuración de interfaces WAN/LAN, WiFi, firewall, DHCP.
- **System:** Estado del sistema (CPU, RAM, storage), logs, backups.
- **Docker:** Gestión de contenedores (vía luci-app-dockerman): start/stop, logs, stats.
- **Services:** Configuración de servicios OpenWRT (dnsmasq, dropbear SSH, uhttpd).

### 5.14.2 Monitoreo de Contenedores

#### Docker Stats

Visualización en tiempo real de recursos por contenedor:

```
docker stats --no-stream
CONTAINER   CPU %    MEM USAGE / LIMIT    MEM %    NET I/O
otbr        2.5%    45MB / 512MB      8.8%    12MB / 8MB
tb-edge     15.3%   320MB / 512MB     62.5%   50MB / 30MB
postgres    5.1%    80MB / 512MB      15.6%   5MB / 5MB
bridge      0.8%    25MB / 512MB      4.9%    8MB / 10MB
```

## Healthchecks

Definir healthchecks en `docker-compose.yml`:

```
services:
  tb-edge:
    healthcheck:
      test: ["CMD", "curl", "-f", "http://localhost:8080/api/health"]
      interval: 30s
      timeout: 10s
      retries: 3
      start_period: 120s
```

Verificar estado:

```
docker ps --filter "health=unhealthy"
```

### 5.14.3 Logs Centralizados

#### Docker Logs

Consulta de logs por contenedor:

```
docker logs -f --tail=100 tb-edge
docker logs --since 1h otbr | grep ERROR
```

#### Syslog Integration

Configurar driver de logging para enviar a syslog remoto:

```
{
  "log-driver": "syslog",
  "log-opt": {
    "syslog-address": "udp://10.0.0.100:514",
    "tag": "gateway-{{.Name}}"
  }
}
```

#### 5.14.4 Backups y Recuperación

##### Backup de Configuración OpenWRT

```
# Backup vía LuCI: System > Backup/Flash Firmware > Generate archive
# O por CLI:
sysupgrade -b /tmp/backup-$(date +%Y%m%d).tar.gz
scp /tmp/backup-* .tar.gz admin@backup-server:/backups/
```

##### Backup de Volúmenes Docker

Script de backup diario (/etc/crontabs/root):

```
#!/bin/sh
# Backup a las 2 AM
0 2 * * * /mnt/docker/scripts/backup.sh

# backup.sh:
DATE=$(date +%Y%m%d)
tar czf /mnt/docker/backups/volumes-$DATE.tar.gz \
  /mnt/docker/tb-edge-data \
  /mnt/docker/postgres-data \
  /mnt/docker/otbr-config

# Retener solo 7 días
find /mnt/docker/backups -name "volumes-* .tar.gz" \
  -mtime +7 -delete
```

##### Disaster Recovery

Procedimiento de recuperación completa:

1. Restaurar OpenWRT: Flash imagen base + restaurar backup de configuración.
2. Montar volumen de datos: `mount /dev/sda1 /mnt/docker`.
3. Restaurar volúmenes Docker desde backup si es necesario.
4. Desplegar contenedores: `docker-compose up -d`.
5. Verificar healthchecks: `docker ps`.
6. Sincronizar TB Edge con cloud: automático al conectar.

## 5.15 Pruebas y Validación

### 5.15.1 Pruebas Funcionales

1. **Formación de red Thread:** Verificar que OTBR forma red y acepta dispositivos comisionados.

```
docker exec -it otbr ot-ctl state # Esperado: "leader"
docker exec -it otbr ot-ctl child table # Listar nodos conectados
```

2. **Conexión HaLow (Morse Micro):** Verificar asociación de DCUs al AP HaLow.

```
iw dev wlan2 station dump # Listar estaciones conectadas
# Esperado: MACs de DCUs con señal >-70 dBm

# Test de throughput HaLow
iperf3 -s & # Servidor en gateway
# En DCU: iperf3 -c <gateway-hallow-ip> -t 60
# Esperado: >20 Mbps promedio
```

3. **Validación Modo AP HaLow:**

```
# Verificar AP activo
iw dev wlan2 info
# Esperado: type AP, channel 7 (917 MHz), width 8 MHz

# Verificar clientes conectados
hostapd_cli -i wlan2 all_sta
# Métricas: signal (dBm), tx_rate (Mbps), rx_rate (Mbps)

# Test QoS: priorizar telemetría (DSCP EF) vs logs (BE)
tc qdisc show dev wlan2
```

4. **Validación Modo STA HaLow:**

```
# Verificar conexión a AP externo
iw dev wlan2 link
# Esperado: Connected to <AP-BSSID>, signal -60 dBm

# Test de failover WAN: STA HaLow como uplink primario
ping -I wlan2 8.8.8.8
# Desconectar AP externo → verificar failover a LTE
```

5. **Validación Modo 802.11s Mesh:**

```
# Verificar mesh formado
iw dev wlan2 station dump
# Esperado: peer mesh STAs con plink_state ESTAB
```

```

# Ver tabla de rutas mesh (HWMP)
iw dev wlan2 mpath dump
# Esperado: rutas a gateways remotos con metric <100

# Test multi-hop: ping desde Gateway A a DCU conectado a Gateway C
ping6 fd00::dcu30 # 2 hops intermedios
# Latencia esperada: <150 ms

# Simulación fallo nodo intermedio
ifdown wlan2 # En Gateway B
# Verificar reconvergencia HWMP (<10s)
# Gateway A re-rutea vía Gateway D (ruta alternativa)

```

#### 6. Validación Modo EasyMesh:

```

# En Controller: verificar topología
ubus call map.controller dump_topology
# Esperado: JSON con Agents y backhaul_link=wlan2

# Test roaming: DCU móvil cambia entre Agent 1 y Agent 2
# Monitorear handoff en Controller
logread -f | grep map-controller
# Esperado: "Steering STA <MAC> from Agent1 to Agent2"
# Latencia handoff <500 ms sin pérdida TCP

# Test band steering: DCU dual-band elige HaLow vs 2.4GHz
# Controller fuerza HaLow si señal >-65 dBm (mayor alcance)

```

#### 7. Prueba Arquitectura Mesh Extendida (3 Gateways):

```

# Topología:
#   [GW-A (0,0)] ---3km--- [GW-B (3km,0)] ---2.5km--- [GW-C (5.5km,0)]
#           |                   |                   |
#   10 DCUs           10 DCUs           10 DCUs

# Test alcance total: ping desde DCU@GW-A a DCU@GW-C
ping6 fd00::dcu25 # 2 hops mesh
# Latencia esperada: <200 ms

# Test failover mesh: desconectar GW-B
# Verificar que GW-A y GW-C mantienen DCUs locales
# pero pierden conectividad inter-gateway (sin ruta alternativa)

# Con 4to gateway (topología redundante):
#   [GW-A] ---[GW-B]--- [GW-C]
#           \       / \   /
#           [GW-D]-----/
# Desconectar GW-B → GW-A y GW-C se comunican vía GW-D

```

#### 8. Failover Ethernet <->LTE: Simular falla de WAN Ethernet.

```
# Desconectar cable Ethernet WAN
ifdown wan_eth

# Verificar conmutación a LTE (<30s)
mwan3 status
ip route show # Esperado: default via LTE (wwan0)

# Reconectar Ethernet
ifup wan_eth
# Verificar restauración automática
```

**9. Publicación MQTT:** Dispositivo Thread publica telemetría y aparece en dashboard TB Edge.

```
# Simular publicación desde bridge
mosquitto_pub -h localhost -p 1883 -u ACCESS_TOKEN \
-t v1/devices/me/telemetry \
-m '{"ts":1730000000000,"values":{"energy_kwh":100.5}}'
```

**10. Sincronización cloud:** Verificar que TB Edge envía datos a TB Cloud.

```
docker logs tb-edge | grep "Cloud synchronization completed"
```

**11. Comando downlink:** Enviar RPC desde TB Cloud y verificar ejecución en dispositivo.

## 5.15.2 Pruebas de Desempeño

**1. Latencia E2E:** Medir tiempo desde publicación en nodo Thread hasta llegada a TB Edge.

- Objetivo: <5 segundos percentil 95.
- Herramienta: timestamps en payload + análisis en TB Edge.

**2. Throughput HaLow:** Máxima capacidad de backhaul DCUs → Gateway.

- Test: 10 DCUs simultáneos @ 2 Mbps c/u = 20 Mbps agregado.
- Métrica: Pérdida de paquetes <0.1% con señal >-65 dBm.
- Rango: Verificar conectividad a 1 km (línea de vista) y 500 m (NLOS con 1 pared).

**3. Throughput MQTT:** Máxima tasa de mensajes sin pérdida.

- Test: 10 dispositivos publicando cada 15 seg = 40 msg/min.
- Escalar hasta observar pérdida o latencia >5s.

**4. Consumo energético:** Medición con PoE meter.

- Idle: <5W (OTBR + TB Edge sin tráfico, LTE idle).
- Carga media: <12W (40 msg/min, HaLow RX, LTE idle).
- Carga alta: <18W (LTE TX activo, límite PoE+ 25W).

**5. Resiliencia offline:** Simular pérdida de conectividad WAN (Ethernet + LTE) durante 24 horas.

- Verificar que TB Edge continúa operando localmente.
- Buffer local debe almacenar >28k mensajes (300 medidores × 96 lecturas/día).
- Al reconectar, confirmar sincronización completa del backlog en <10 min.

**6. Tiempo de failover WAN:** Medir latencia de conmutación Ethernet → LTE.

- Ping continuo a 8.8.8.8 durante test.
- Desconectar Ethernet, medir tiempo hasta recuperación de ping vía LTE.
- Objetivo: <30 segundos (incluyendo renegociación TCP).

### 5.15.3 Pruebas de Seguridad

**1. Firewall:** Escaneo de puertos con nmap desde WAN.

```
nmap -sS -p- <gateway-wan-ip>
# Esperado: Solo puertos explicitamente abiertos (ej. 22 SSH, 443 HTTPS)
```

**2. Seguridad HaLow WPA3-SAE:** Validar que PMF (Protected Management Frames) está activo.

```
iw dev wlan2 info | grep "PMF"
# Esperado: "PMF: required"

# Intentar asociación con estación sin WPA3
wpa_supplicant -i wlan1 -c /tmp/wpa2-only.conf
# Esperado: Association rejected (WPA3 required)
```

**3. TLS/mTLS:** Validar certificados con openssl.

```
openssl s_client -connect <tb-cloud>:7070 -CAfile ca.crt
# Verificar: Verify return code: 0 (ok)
```

**4. Inyección MQTT:** Intentar publicar sin autenticación.

```
mosquitto_pub -h localhost -p 1883 -t test -m "unauthorized"
# Esperado: Connection refused o Authentication failed
```

**5. Container escape:** Verificar que contenedores no tienen acceso privilegiado innecesario.

```
docker inspect tb-edge | grep '"Privileged": false'
# Excepto OTBR que requiere host network para RCP
```

**6. LTE APN security:** Validar que credenciales APN no están en logs.

```
grep -r "apn.*password" /var/log/
# Esperado: Sin resultados (credenciales cifradas en uci)
```

**7. Actualizaciones automáticas:** Confirmar que Watchtower actualiza imágenes vulnerables.

```
docker logs watchtower | grep "Updated"
```

#### 5.15.4 Pruebas de Integración

1. **Comisionado Thread:** Agregar nuevo dispositivo vía OTBR web UI.
2. **Reglas TB Edge:** Crear regla de alarma por consumo >5 kW, verificar activación.
3. **Dashboard en tiempo real:** Visualizar telemetría con latencia <2s en interfaz web.
4. **API REST:** Consultar dispositivos y telemetría vía API de TB Edge.

```
curl -X GET http://localhost:8080/api/tenant/devices \
      -H "X-Authorization: Bearer $TOKEN"
```

5. **Resiliencia offline:** Simular desconexión WAN durante 24h, verificar queue y sincronización.

```
# Desconectar WAN
ifdown wan_eth wan_lte

# Generar telemetría durante 24h (28,800 mensajes @ 1 msg/3s)
for i in {1..28800}; do
    mosquitto_pub -h localhost -p 1883 -u TOKEN \
        -t v1/devices/me/telemetry \
        -m "{\"ts\":$(date +%s)000,\"values\":{\"energy\":$RANDOM}}"
    sleep 3
done

# Verificar queue size
du -sh /mnt/ssd/docker/queue
# Esperado: ~150-200 MB con compresión

# Reconectar WAN
ifup wan_eth

# Monitorear catch-up sync
docker logs -f tb-edge | grep "Syncing batch"
# Esperado: 100k msgs sincronizados en <15 min
```

### 5.16 Integración de Inteligencia Artificial con MCP y LLM

#### 5.16.1 Arquitectura de IA en el Gateway

El gateway soporta integración de **modelos de lenguaje (LLM)** y **Model Context Protocol (MCP)** para análisis avanzado de telemetría y mantenimiento predictivo:

- **MCP (Model Context Protocol):** Protocolo estándar para comunicación entre aplicaciones y servicios de IA (Claude, GPT, modelos locales).

## 5.16. Integración de Inteligencia Artificial con MCP y LLM 5. Gateway de Telemetría para Smart Energy

- **LLM local (Ollama)**: Modelos open-source ejecutándose en gateway (Llama 3.2, Mistral, Phi-3).
- **ThingsBoard Edge + IA**: Integración vía Rule Engine para análisis en tiempo real.

### 5.16.2 Model Context Protocol (MCP)

**MCP** es un protocolo abierto desarrollado por Anthropic que permite a aplicaciones:

- Conectarse a múltiples proveedores de IA (Claude, OpenAI, Azure OpenAI, modelos locales).
- Proporcionar contexto estructurado a modelos (herramientas, datos, prompts).
- Ejecutar acciones en sistemas externos desde respuestas de LLM.

**Componentes MCP**:

1. **MCP Server**: Expone herramientas y recursos al LLM (ej. consultar TB Edge API).
2. **MCP Client**: Aplicación que consume servicios de IA (ej. dashboard analítico).
3. **Protocolo**: JSON-RPC 2.0 sobre stdio/SSE/WebSocket.

### 5.16.3 Despliegue de Ollama (LLM Local)

Ollama permite ejecutar modelos LLM localmente sin enviar datos a cloud externo:

#### Instalación en Gateway

Docker Compose para Ollama:

```
# /mnt/ssd/docker/ollama/docker-compose.yml
version: '3.8'
services:
  ollama:
    image: ollama/ollama:latest
    container_name: ollama
    ports:
      - "11434:11434" # API REST
    volumes:
      - ./models:/root/.ollama
```

## 5. Gateway de Telemetría para Smart Energy 5.16. Integración de Inteligencia Artificial con MCP y LLM

```
environment:
  - OLLAMA_HOST=0.0.0.0
restart: unless-stopped
# Requiere GPU (opcional) o CPU (8 GB RAM mínimo)
deploy:
  resources:
    limits:
      memory: 8G
```

Desplegar y descargar modelo:

```
cd /mnt/ssd/docker/ollama
docker-compose up -d

# Descargar modelo Llama 3.2 (3B parámetros, 2 GB)
docker exec -it ollama ollama pull llama3.2:3b

# O modelo Phi-3 (mini, 1.3 GB, optimizado para edge)
docker exec -it ollama ollama pull phi3:mini
```

Prueba de inferencia:

```
curl http://localhost:11434/api/generate -d '{
  "model": "llama3.2:3b",
  "prompt": "Analiza este patrón de consumo: 100 kWh, 120 kWh, 150 kWh, 200 kWh. ¿Es anómalo?",
  "stream": false
}'
```

### 5.16.4 MCP Server para ThingsBoard Edge

Implementación de MCP Server que expone API de TB Edge al LLM:

#### Código MCP Server (Python)

Archivo /mnt/ssd/docker/mcp-server/tb\_mcp\_server.py:

```
#!/usr/bin/env python3
import json
import sys
from typing import Any
import requests
```

```
# MCP Server para TB Edge
class TBEdgeMCPServer:
    def __init__(self, tb_url="http://tb-edge:8080", token ""):
        self.tb_url = tb_url
        self.token = token

    def get_device_telemetry(self, device_id: str, keys: str,
                           start_ts: int, end_ts: int):
        """Obtiene telemetría de dispositivo"""
        url = f"{self.tb_url}/api/plugins/telemetry/DEVICE/{device_id}/values/timeseries"
        params = {"keys": keys, "startTs": start_ts, "endTs": end_ts}
        headers = {"X-Authorization": f"Bearer {self.token}"}

        resp = requests.get(url, params=params, headers=headers)
        return resp.json()

    def get_device_alarms(self, device_id: str):
        """Obtiene alarmas activas de dispositivo"""
        url = f"{self.tb_url}/api/alarm/DEVICE/{device_id}"
        headers = {"X-Authorization": f"Bearer {self.token}"}

        resp = requests.get(url, headers=headers)
        return resp.json()

    def handle_mcp_request(self, request: dict) -> dict:
        """Procesa solicitud MCP JSON-RPC 2.0"""
        method = request.get("method")
        params = request.get("params", {})

        if method == "tools/list":
            return {
                "tools": [
                    {
                        "name": "get_device_telemetry",
                        "description": "Obtiene telemetría histórica de dispositivo",
                        "inputSchema": {
                            "type": "object",
                            "properties": {
                                "device_id": {"type": "string"},
                                "keys": {"type": "string"},
                                "start_ts": {"type": "integer"},
                                "end_ts": {"type": "integer"}
                            }
                        }
                    }
                ],
                {
                    "name": "get_device_alarms",
                    "description": "Obtiene alarmas activas de dispositivo",
                    "inputSchema": {
                        "type": "object",
                        "properties": {
                            "device_id": {"type": "string"}
                        }
                    }
                }
            }
```

```

        }
    ]
}

elif method == "tools/call":
    tool_name = params.get("name")
    tool_args = params.get("arguments", {})

    if tool_name == "get_device_telemetry":
        result = self.get_device_telemetry(**tool_args)
        return {"content": [{"type": "text", "text": json.dumps(result)}]}

    elif tool_name == "get_device_alarms":
        result = self.get_device_alarms(**tool_args)
        return {"content": [{"type": "text", "text": json.dumps(result)}]}

    return {"error": "Unknown method"}

def run(self):
    """Loop principal MCP stdio"""
    for line in sys.stdin:
        try:
            request = json.loads(line)
            response = self.handle_mcp_request(request)
            response["id"] = request.get("id")
            print(json.dumps(response), flush=True)
        except Exception as e:
            print(json.dumps({"error": str(e)}), file=sys.stderr, flush=True)

if __name__ == "__main__":
    server = TBEedgeMCPServer(token="YOUR_TB_TOKEN")
    server.run()

```

## Configuración MCP Client

Archivo de configuración MCP (`mcp_config.json`):

```
{
  "mcpServers": {
    "thingsboard-edge": {
      "command": "python3",
      "args": ["/mnt/ssd/docker/mcp-server/tb_mcp_server.py"],
      "env": {
        "TB_URL": "http://tb-edge:8080",
        "TB_TOKEN": "YOUR_ACCESS_TOKEN"
      }
    }
  }
}
```

### 5.16.5 Casos de Uso de IA en Gateway

#### Análisis de Anomalías en Consumo

Prompt al LLM vía MCP:

"Analiza el consumo energético del medidor METER-001 en las últimas 24 horas. Identifica patrones anómalos que puedan indicar fraude, falla del medidor o consumo irregular. Proporciona recomendaciones."

Flujo:

1. LLM invoca `get_device_telemetry` vía MCP para obtener datos.
2. Analiza serie temporal (100 puntos, intervalo 15 min).
3. Detecta pico de 500 kWh a las 3 AM (vs promedio 50 kWh).
4. Genera respuesta: "Anomalia detectada: consumo 10x superior al promedio. Posible bypass del medidor o falla de CT (transformador de corriente). Recomendar inspección física."

#### Mantenimiento Predictivo

Prompt:

"Evalúa el estado de los 50 medidores en la zona Norte. Predice cuáles tienen mayor probabilidad de falla en los próximos 30 días basándose en alarmas históricas, lecturas inconsistentes y tiempo de operación."

LLM:

1. Consulta alarmas de 50 dispositivos (`get_device_alarms`).
2. Identifica 5 medidores con >10 alarmas en 7 días.
3. Analiza telemetría: lecturas con alta varianza o valores fuera de rango.
4. Genera ranking de prioridad de mantenimiento.

### Asistente de Operación (Chatbot)

Dashboard TB Edge con chatbot integrado:

Usuario: "¿Cuántos medidores están offline en este momento?"

LLM: [Consulta TB Edge API] "Actualmente 3 medidores offline:  
METER-042, METER-089, METER-123. Última comunicación hace  
2 horas. Posible problema de conectividad Thread."

Usuario: "¿Cuál es el consumo total del edificio hoy?"

LLM: [Suma telemetría de 50 medidores] "Consumo total: 1,250 kWh  
(hasta las 14:30). Proyección diaria: 2,100 kWh, 15% superior  
al promedio semanal."

### 5.16.6 Ventajas de IA Local (Ollama + MCP) vs Cloud

Característica	IA Local (Gateway)	IA Cloud (GPT-4/Claude)
Latencia	<500 ms	2-5 segundos
Privacidad datos	Alta (no salen del gateway)	Baja (envío a cloud)
Costo operación	\$0 (hardware local)	\$0.01-0.10/consulta
Disponibilidad offline	100 %	0 % (requiere internet)
Modelos disponibles	Open-source (Llama, Phi)	Propietarios (GPT, Claude)
Capacidad análisis	Media (3B-7B params)	Alta (100B+ params)
Consumo energético	+5W (CPU) / +15W (GPU)	N/A

Tabla 5-9: Comparación IA local vs cloud para gateway Smart Energy

**Recomendación:** Usar IA local (Ollama + MCP) para análisis en tiempo real y privacidad, reservar IA cloud para análisis complejos periódicos (tendencias mensuales, optimización de red).

## 5.17 Conclusiones del Capítulo

El gateway basado en OpenWRT con arquitectura de contenedores Docker y conectividad multiradio (HaLow + LTE) ofrece ventajas significativas para despliegues de telemetría Smart Energy:

- **Flexibilidad:** Contenedores Docker permiten actualizar, escalar y modificar servicios independientemente sin afectar el sistema base.
- **Edge Computing:** ThingsBoard Edge procesa datos localmente (reglas, alarmas, dashboards) reduciendo latencia y dependencia del cloud.
- **Conectividad robusta multimodal (HaLow + LTE):**
  - **802.11ah (Morse Micro MM6108):** Backhaul de largo alcance (1-3 km) y alta estabilidad para DCUs con throughput de hasta 40 Mbps, consumo <500 mW y certificaciones industriales (-40°C a +85°C).

- **Modos HaLow avanzados:**

- **AP:** Cobertura centralizada 3 km, topología estrella simple.
- **STA:** Cliente para backhaul rural sin costo celular recurrente.
- **802.11s Mesh:** Auto-healing, extensión 6-9 km con 2-3 gateways, routing automático HWMP.
- **EasyMesh:** Roaming transparente, gestión centralizada, steering inteligente de clientes.

- **LTE Cat-6 (M.2):** Uplink redundante con failover automático <30s, ideal para zonas sin infraestructura fija. Optimización de costos con compresión CBOR (40-60 % reducción) y batching inteligente.

- **Failover automático:** Política de métricas de ruta (Ethernet metric=10, LTE metric=20) con monitoreo activo vía mwan3.

- **Escalabilidad Arquitectónica con Mesh HaLow:**

- **Topología estrella (AP único):** 10 DCUs × 250 nodos Thread = 2,500 endpoints, cobertura 3 km, latencia <50 ms.
- **Topología mesh (3 gateways 802.11s):** 30 DCUs × 250 nodos = 7,500 endpoints, cobertura 9 km, latencia <200 ms, resiliencia ante fallo de gateway.
- **Topología EasyMesh (1 Controller + 4 Agents):** 50 DCUs × 250 nodos = 12,500 endpoints, roaming transparente, carga balanceada automática.

- **Reducción CAPEX/OPEX con Arquitectura Mesh:**

- **CAPEX:** 3 gateways con mesh HaLow backhaul vs. 9 gateways con uplink dedicado (fibra/LTE) para misma cobertura (9 km) = ahorro 66 % en infraestructura WAN.
- **OPEX:** Backhaul HaLow sin costo recurrente vs. 9 planes LTE × \$30/mes = ahorro \$3,240/año.
- **Instalación:** Mesh auto-configura rutas vs. despliegue manual de enlaces backhaul = reducción 40 % tiempo de instalación.

- **Interoperabilidad:** OpenThread Border Router gestiona redes Thread mesh con soporte estándar Thread 1.3, compatible con múltiples fabricantes de dispositivos IoT.

- **Resiliencia:**

- **SSD NVMe:** Almacenamiento persistente de alta durabilidad (>1M ciclos E/W, >3000 IOPS) para PostgreSQL y queue TB Edge.
- **Queue persistente:** Hasta 100k mensajes offline (2 GB, 7 días @ 300 medidores), sincronización acelerada en <15 min (batch 5000 msgs).
- **Protección multivel:** 6 capas de resiliencia (hardware, filesystem, DB, aplicación, red, containers) con RTO <5 min.
- **Compresión inteligente:** gzip/lz4 reduce queue 40-60 %, eliminación automática de telemetría >7 días.
- Redundancia WAN con conmutación transparente para aplicaciones.
- **Mesh auto-healing:** Reconvergencia HWMP <10s ante fallo de nodo intermedio, eliminando single point of failure.

- **Inteligencia Artificial (Roadmap Futuro):**

- **MCP (Model Context Protocol):** Estándar abierto Anthropic para integración de LLMs con TB Edge API, permitiendo análisis avanzado de telemetría vía herramientas estructuradas.
- **Ollama local (planeado):** Modelos open-source (Llama 3.2 1B, Phi-3 mini) ejecutando en gateway con latencia <500 ms, privacidad 100 % (datos no salen del gateway). Requiere optimización térmica adicional en Raspberry Pi 4 (ventilador activo, heatsink GPU).

- **Casos de uso potenciales:** Detección de anomalías (fraude, bypass CT), mantenimiento predictivo (ranking de medidores con mayor riesgo de falla), chatbot operacional (consultas en lenguaje natural sobre telemetría).
- **Limitación actual:** Raspberry Pi 4 con 4 GB RAM solo permite modelos <3 GB (Llama 3.2 1B, Phi-3 mini 1.3 GB) para mantener recursos para PostgreSQL/Kafka/TB Edge. Versión 8 GB recomendada para IA en producción.
- **Alternativa:** MCP client conectado a Ollama en servidor dedicado (no en gateway) para análisis batch offline de datos históricos exportados desde PostgreSQL.

■ **Arquitectura de Datos Distribuida:**

- **Apache Kafka:** Message broker distribuido, >100k msg/s, buffer persistente 7 días, multi-consumidor (TB Edge + analítica + ML), compresión gzip, backpressure handling.
- **PostgreSQL + TimescaleDB:** Series temporales optimizadas, compresión 10-20×, particionamiento automático, retención 90 días, queries agregadas (time\_bucket), hypertables con >3000 IOPS en SSD NVMe.
- **Ventajas Kafka:** Replay histórico, desacoplamiento productor/consumidor, tolerancia a picos de tráfico (GB de buffer vs 100k msgs in-memory).

■ **Protocolos de Comunicación IoT Multiprotocolo:**

- **MQTT (QoS 0/1/2):** Telemetría uplink (medidor→gateway), Pub/Sub desacoplado, LWT para detección de desconexión, retained messages, broker Mosquitto con TLS/mTLS.
- **CoAP (UDP):** Thread mesh intra-nodo, 4 bytes overhead vs 100+ HTTP, Observe para suscripciones, DTLS+PSK, block-wise transfer, RESTful methods (GET/POST/PUT/DELETE).
- **HTTP/REST:** APIs gestión (TB Edge, IEEE 2030.5, LuCI, Ollama), webhooks, integraciones cloud.
- **LwM2M:** Device management (bootstrap, firmware OTA), objetos estándar OMA (3305 Power Measurement), operaciones Read/Write/Execute/Observe, DTLS eficiente (PSK 16 bytes vs X.509 2 KB).
- **Selección inteligente:** MQTT QoS 1 para telemetría crítica, CoAP para Thread mesh, LwM2M para firmware OTA, HTTP para IEEE 2030.5 SEP 2.0.

■ **Seguridad multicapa:**

- Firewall nftables a nivel de sistema operativo.
- Aislamiento de contenedores con namespaces de kernel.
- TLS/mTLS para comunicaciones cloud (puerto 7070 gRPC).
- Thread AES-128-CCM para red de campo.
- HaLow WPA3-SAE con PMF obligatorio (Morse Micro), protección mesh con SAE authentication en 802.11s.
- **OpenVPN:** Túnel VPN permanente para acceso remoto seguro al gateway (SSH, LuCI, logs) desde NOC sin exponer puertos a internet.

■ **Mantenibilidad y Gestión Centralizada:**

- **OpenWRT Feeds:** Gestión de paquetes con opkg (update/install/upgrade), feeds oficiales (packages, luci, routing) + custom feed para paquetes Smart Grid propietarios, actualización masiva de dependencias.
- **OpenVPN:** Acceso remoto seguro vía túnel VPN permanente (hub-spoke architecture), IPs fijas por gateway (10.8.0.100-199), client-to-client para troubleshooting inter-gateway, certificados PKI (CA + client certs), keepalive para detección de desconexión <120s.

- **OpenWISP:** Plataforma centralizada para gestión masiva (100-1000 gateways), templates UCI con variables ({{apn}}, {{halow\_channel}}), push configuración remota vía HTTPS, Firmware OTA scheduler con dual-partition rollback, monitoring (CPU/RAM/Storage/Interfaces/Docker), alertas (email/SMS/webhook), zero-touch provisioning.
  - Actualizaciones OTA de contenedores con Watchtower.
  - Backups automatizados de configuración y volúmenes Docker.
  - Monitoreo centralizado vía logs, healthchecks y vnstat.
  - **EasyMesh:** Configuración remota de todos los Agents desde Controller único.
- **Escalabilidad:** Soporta hasta 10 DCUs simultáneos vía HaLow AP (cada DCU con 250 nodos Thread) con agregación en TB Edge antes de enviar al cloud. Mesh y EasyMesh multiplican capacidad 3-5× sin rediseño arquitectónico.
- **Costo-efectividad:**
- Hardware de propósito general (router OpenWRT + módulos M.2 estándar) reduce CAPEX vs. gateways propietarios.
  - Optimización LTE reduce OPEX: 3.7 GB/mes promedio vs. 20-30 GB sin compresión.
  - Mesh HaLow elimina necesidad de backhaul dedicado en 60-70 % de nodos.
- **Conformidad con Estándares Internacionales:**
- **IEEE 2030.5-2023:** Soporte completo de Function Sets (DCAP, TM, MM, MSG, ED) con API REST XML, autenticación X.509 ECC P-256, LFDI, RBAC.
  - **ISO/IEC 30141:2024:** Arquitectura IoT de referencia con 4 vistas (funcional, información, despliegue, operacional) cubriendo 8 entidades funcionales.
  - Cumplimiento regulatorio CREG (Colombia) para medición inteligente y Smart Energy Profile 2.0 para interoperabilidad con utilidades.

### 5.17.1 Casos de Uso Óptimos por Modo HaLow

Modo	Escenario	Ventajas Clave	Ejemplo Despliegue
AP (Router)	Zona urbana densa	Control total, simplicidad, baja latencia	1 gateway por edificio (300 medidores, <1 km)
AP (Bridge)	Integración con LAN existente	Transparencia L2, DHCP unificado	Campus con switches Ethernet, gateway como AP bridge
STA	Zona rural sin fibra/LTE	Ahorro OPEX, throughput alto	Gateway conecta a torre utilidad con HaLow AP (10 km)
802.11s Mesh	Área extendida sin infraestructura	Auto-healing, 3x cobertura, CAPEX reducido	3 gateways mesh en zona rural (9 km, 900 medidores)
EasyMesh	Multi-edificio/campus	Roaming, gestión centralizada, QoS	Universidad con 5 edificios, 1 Controller + 4 Agents

Tabla 5-10: Casos de uso óptimos por modo de operación HaLow

Característica	Morse Micro MM6108	Newracom NRC7292	Qualcomm QCA8081
Alcance típico	<b>3 km</b>	1.5 km	1 km
Throughput máximo	<b>40 Mbps</b>	32 Mbps	24 Mbps
Consumo TX	<b>&lt;500 mW</b>	800 mW	1 W
Drivers Linux	<b>Mainline (ath11k)</b>	Out-of-tree	Propietario
Temp. operación	-40°C a +85°C	-20°C a +70°C	-10°C a +60°C
Certificaciones	FCC/CE/IC	FCC/CE	FCC
Soporte Mesh 802.11s	<b>Sí (ath11k nativo)</b>	Limitado	No
EasyMesh (IEEE 1905.1)	Sí	Beta	No
Costo (qty 100)	\$12	\$15	\$18

Tabla 5-11: Comparación de soluciones HaLow comerciales (2025)

### 5.17.2 Ventajas de Morse Micro sobre Alternativas HaLow

### 5.17.3 Limitaciones y Trabajo Futuro

#### ■ Validación de Performance (Pendiente):

- Mediciones CPU/RAM bajo carga completa (OTBR + TB Edge + PostgreSQL + Kafka) con herramientas como `htop`, `docker stats`, `sysbench`.
- Benchmarks de temperatura operativa (idle vs carga) con ventilador PoE HAT activo, objetivo <75°C bajo carga sostenida.
- Test de throughput E2E: nodo Thread → OTBR → HaLow → TB Edge → PostgreSQL con `iperf3` y latencia con `ping6`.
- Stress test: 1000 msg/s durante 24h para validar estabilidad térmica y resiliencia del SSD NVMe.

#### ■ Conectividad HaLow vía USB (Roadmap):

- Morse Micro planea soporte USB 2.0 High-Speed (Q2 2026) para simplificar integración.
- Conexión USB elimina complejidad SPI (IRQ handling, clock sync) y permite hot-plug.
- Validar drivers `ath11k_usb` en OpenWRT 24.x cuando estén disponibles.

#### ■ Inteligencia Artificial Local:

- Desplegar Ollama con modelo Llama 3.2 1B (2 GB) o Phi-3 mini (1.3 GB) en Raspberry Pi 4 de 8 GB RAM.
- Implementar MCP Server Python para exponer TB Edge API como herramientas estructuradas (`get_device_telemetry`, `get_device_alarms`).
- Validar casos de uso: detección de anomalías (fraude, bypass CT), mantenimiento predictivo (ranking dispositivos con alarmas).
- Alternativa: Ollama en servidor x86 dedicado para análisis batch offline de datos históricos PostgreSQL.

#### ■ Rendimiento I/O: SSD NVMe M.2 (256 GB) proporciona >3000 IOPS medidos, suficiente para PostgreSQL + Kafka. Para >500 dispositivos considerar RAID-1 NVMe para redundancia (requiere Compute Module 4 con dual M.2).

#### ■ Alta disponibilidad: Implementar par de gateways Raspberry Pi 4 en activo-pasivo con VRRP/keepalived para redundancia completa. En topología mesh, configurar 2 gateways con uplink LTE como root bridges redundantes con RSTP (Rapid Spanning Tree Protocol).

■ **Raspberry Pi vs Hardware Industrial:**

- Evaluar migración a Raspberry Pi Compute Module 4 (CM4) con carrier board industrial (DIN-rail mount, -40°C a +85°C, dual Ethernet, dual M.2 NVMe).
  - Ventajas CM4: PCIe nativo (no HAT), más compacto, certificaciones industriales (vibración, EMI/EMC).
  - Alternativa: Hardware x86 industrial (Intel Atom, Celeron N5105) con 8 GB RAM, dual NIC, PCIe, pero mayor costo (\$200-300 vs \$55 RPi 4).
- **5G RedCap:** Evaluar migración de Quectel BG95 (LTE-M) a módulos 5G Reduced Capability (Quectel RG500U) para menor latencia (<50ms vs 100-300ms) y mayor throughput (100 Mbps vs 375 kbps), crítico para comandos RPC downlink en tiempo real.
- **Agregación de enlaces:** Implementar MPTCP (Multipath TCP) para utilizar Ethernet + LTE simultáneamente, aumentando throughput y resiliencia con failover <1s sin pérdida de conexiones TCP activas.
- **Mesh avanzado:** Explorar fastroaming 802.11r en EasyMesh para handoff <50ms (crítico para vehículos eléctricos en movimiento con carga dinámica V2G).
- **HaLow + LoRaWAN híbrido:** Evaluar integración de LoRaWAN (915 MHz) para sensores ultra-low-power (<10 mW, batería 10 años) con HaLow como backhaul de gateways LoRa concentradores (Semtech SX1302).
- **Quantum-safe crypto:** Preparar migración a algoritmos post-cuánticos (Kyber-768, Dilithium-3) en certificados X.509 para protección a largo plazo (NIST PQC Round 4, 2025+), especialmente crítico para infraestructura crítica Smart Grid con vida útil >20 años.

**Próximo capítulo:** Se presentará la arquitectura completa del sistema de telemetría, integrando los nodos Thread (ESP32-C6), DCUs con Thread Border Router, el gateway Raspberry Pi 4 + OpenWRT con HaLow multimodal (AP/STA/Mesh/EasyMesh), Quectel BG95 LTE-M y nRF52840 Thread RCP, y la plataforma cloud ThingsBoard, con un caso de estudio de despliegue real para 900 medidores residenciales en infraestructura colombiana con topología mesh 802.11s (3 gateways × 9 km cobertura).

# 6 Arquitectura de Telemetría para Smart Energy

## 6.1 Introducción

Este capítulo presenta la arquitectura completa del sistema de telemetría propuesto para aplicaciones de Smart Energy, integrando los componentes descritos en el capítulo anterior (Gateway) en una solución end-to-end escalable y segura.

## 6.2 Visión General de la Arquitectura

### 6.2.1 Componentes Principales

La arquitectura se compone de cuatro capas principales:

1. **Capa de Dispositivos:** Medidores inteligentes con interfaces DLMS/COSEM.
2. **Capa de Campo (Field Network):** Nodos adaptadores 802.15.4/Thread y DCUs (Thread Border Routers).
3. **Capa de Agregación (Backhaul):** Gateway con uplink 802.11ah/HaLow y WiFi.
4. **Capa de Aplicación (Cloud):** Plataforma IoT (ThingsBoard) con analytics y visualización.

**Figura 6-1:** Arquitectura completa del sistema de telemetría

## 6.3 Capa de Dispositivos: Medidores Inteligentes

### 6.3.1 Características de los Medidores

- Cumplimiento IEC 62052/62053 (clase 1 o 2 según precisión).
- Interfaz DLMS/COSEM sobre RS-485 o puerto óptico IEC 62056-21.
- Registro de perfiles de carga, eventos y parámetros instantáneos (OBIS).
- Opcional: detección de manipulación (tamper), corte/reconexión remota.

### 6.3.2 Interfaz de Lectura

Cada medidor expone:

- **Perfiles de carga:** Histórico de consumo con resolución configurable (15 min típica).
- **Registros instantáneos:** Tensión, corriente, potencia activa/reactiva, factor de potencia.
- **Eventos:** Cortes de suministro, sobretensión, tamper magnético/físico.

## 6.4 Capa de Campo: Nodos y DCUs

### 6.4.1 Nodos Adaptadores RS485 + ESP32C6 + Thread

#### Función

Actúan como puente entre el medidor (RS-485) y la red Thread (802.15.4):

- Lectura periódica del medidor vía DLMS/COSEM.
- Encapsulación de datos en paquetes IPv6/6LoWPAN.
- Transmisión a DCU (Thread Border Router) por radio 802.15.4.

## Hardware

- **MCU:** ESP32C6 (radio 802.15.4 integrado).
- **Transceptor RS-485:** MAX485 o SP485 con aislamiento galvánico.
- **Alimentación:** 5V desde medidor (si disponible) o batería + supercap.
- **Antena:** PCB o externa para 2.4 GHz (Thread).

## Software

- Stack Thread (OpenThread en ESP-IDF).
- Cliente DLMS simplificado (lectura de OBIS configurables).
- Sleep modes para optimizar consumo energético.

### 6.4.2 DCU (Data Concentrator Unit)

#### Función

El DCU cumple roles críticos:

1. **Thread Border Router:** Termina red Thread y conecta a IP (WiFi/Ethernet).
2. **Agregador de datos:** Recibe lecturas de hasta 100 nodos Thread por DCU.
3. **Preprocesamiento:** Validación, filtrado de duplicados, compresión.
4. **Uplink:** Transmite datos agregados al Gateway por 802.11ah.

## Hardware

- **MCU:** ESP32C6 (dual radio: Thread + WiFi).
- **Módulo HaLow:** Newracom NRC7292 o similar (SPI/SDIO).
- **Alimentación:** PoE 802.3af (13W) o AC/DC con batería de respaldo.
- **Almacenamiento:** SD card opcional para buffer extendido.

- Thread Border Router (OpenThread Border Router - OTBR).
- Stack WiFi (ESP-IDF native).
- Driver HaLow (vendor SDK integrado en FreeRTOS).
- Cola de mensajes con persistencia en SPIFFS/SD.

## 6.5 Topología de Red Thread

### 6.5.1 Mesh Networking

Thread implementa una red mallada auto-organizante:

- **Leader:** Un nodo coordina la red (elegido automáticamente).
- **Routers:** Nodos que enrutan tráfico de otros nodos.
- **End Devices:** Nodos de bajo consumo (ej. nodos adaptadores de medidor).

### 6.5.2 Ventajas de Thread

- Auto-healing: Si un nodo falla, la red se auto-reconfigura.
- IPv6 nativo: Direccionamiento global único para cada nodo.
- Seguridad: AES-128 CCM en capa de enlace, DTLS en capa de aplicación.
- Escalabilidad: Hasta 250+ nodos por red Thread.

### 6.5.3 Configuración de Red

- **Channel:** 2.4 GHz, canal 15-26 (evitar interferencia WiFi).
- **PAN ID:** Identificador único de red Thread.
- **Network Key:** Llave de 128 bits compartida (preconfigurada o commissioning).

## 6.6 Backhaul: 802.11ah (HaLow)

### 6.6.1 Justificación de HaLow

HaLow (802.11ah) ofrece ventajas sobre WiFi tradicional:

- **Alcance:** Hasta 1 km en línea de vista (vs. 100m WiFi 2.4 GHz).
- **Penetración:** Mejor propagación en interiores (banda sub-1 GHz).
- **Consumo:** Modos de ahorro energético (TIM, RAW).
- **Densidad:** Soporte de miles de clientes por AP.

### 6.6.2 Configuración HaLow

- **Banda:** 902-928 MHz (ISM, región dependiente).
- **Ancho de canal:** 1-8 MHz (configurable según regulación).
- **Seguridad:** WPA3-SAE (autenticación resistente a diccionario).
- **QoS:** WMM para priorizar tráfico de telemetría crítica.

### 6.6.3 Topología HaLow

- **Gateway como AP:** El gateway actúa como Access Point HaLow.
- **DCUs como clientes:** Hasta 10 DCUs asociados al gateway simultáneamente.
- **Alternat:** Mesh HaLow (si módulos soportan) para mayor cobertura.

## 6.7 Gateway y Uplink a Cloud

(Ver Capítulo 3 para detalles del Gateway)

### 6.7.1 Resumen de Funciones

- Recepción de datos de DCUs por 802.11ah.
- Normalización y agregación.
- Publicación MQTT/TLS a ThingsBoard (puerto 8883).
- Buffer offline y reconexión automática.

## 6.8 Capa de Aplicación: ThingsBoard

### 6.8.1 Funcionalidades

- **Ingesta de telemetría:** Suscripción a topics MQTT, persistencia en base de datos.
- **Visualización:** Dashboards en tiempo real con gráficos de consumo, alarmas.
- **Reglas y alertas:** Detección de anomalías (consumo excesivo, caída de tensión).
- **API REST:** Integración con sistemas externos (facturación, ERP).
- **Control remoto:** Comandos de corte/reconexión hacia medidores (downlink).

### 6.8.2 Modelo de Datos en ThingsBoard

#### Entidades

- **Device:** Cada medidor es un dispositivo con ID único.
- **Asset:** Grupo lógico de medidores (ej. por transformador, zona geográfica).
- **Customer:** Cliente/usuario final que consulta su consumo.

#### Atributos y Telemetría

- **Atributos:** Metadatos estáticos (ubicación, tipo de medidor, tarifa).
- **Telemetría:** Series temporales de consumo, tensión, corriente, etc.

## 6.9 Caso de Estudio: Despliegue en Smart Energy

### 6.9.1 Escenario

Despliegue en zona residencial de 300 viviendas, divididas en 3 sectores:

- **Sector 1:** 100 medidores conectados a DCU-1.
- **Sector 2:** 100 medidores conectados a DCU-2.
- **Sector 3:** 100 medidores conectados a DCU-3.
- **Gateway:** Ubicado en punto central con línea de vista a los 3 DCUs.

### 6.9.2 Dimensionamiento

#### Tráfico Esperado

- Lecturas cada 15 minutos: 96 lecturas/día/medidor.
- 300 medidores: 28,800 lecturas/día.
- Tamaño por mensaje: 200 bytes (JSON).
- Tráfico diario: ~5.5 MB/día (carga muy baja).

#### Capacidad de Red

- **Thread:** 250 kbps efectivos, soporta 100 nodos por DCU con holgura.
- **HaLow (1 MHz, MCS0):** 150 kbps, suficiente para 3 DCUs.
- **WiFi uplink:** 54 Mbps (802.11g mínimo), no es cuello de botella.

### 6.9.3 Resiliencia y Redundancia

- **DCU:** Buffer local de 48h (SD card).
- **Gateway:** Buffer local de 24h (flash).
- **ThingsBoard:** Replicado con PostgreSQL HA (3 nodos).

#### 6.9.4 Seguridad End-to-End

Tramo	Mecanismo de Seguridad
Medidor → Nodo	DLMS HLS (AES-GCM)
Nodo → DCU (Thread)	AES-128 CCM + DTLS
DCU → Gateway (HaLow)	WPA3-SAE
Gateway → ThingsBoard	MQTT/TLS 1.3 (mTLS)

Tabla 6-1: Seguridad por capa

## 6.10 Análisis de Costos

### 6.10.1 Costos de Hardware (estimado)

Componente	Cantidad	Precio Unit.	Total
Nodo (ESP32C6 + RS485)	300	\$15	\$4,500
DCU (ESP32C6 + HaLow)	3	\$80	\$240
Gateway (ESP32C6 + HaLow)	1	\$100	\$100
ThingsBoard (cloud)	1	\$50/mes	\$600/año
<b>Total</b>			<b>\$5,440 + \$600/año</b>

Tabla 6-2: Costos de implementación

### 6.10.2 Comparación con Alternativas

- **Celular (NB-IoT)**: \$10/mes/dispositivo = \$36,000/año (inviable).
- **PLC (G3-PLC/PRIME)**: Mayor costo de nodos (\$30-40), sin ventajas claras.
- **LoRaWAN**: Mayor latencia (clase A), menor throughput, similar alcance.

## 6.11 Métricas de Desempeño

### 6.11.1 Latencia E2E

- **Medidor → ThingsBoard**: <5 segundos (promedio 3s medido en piloto).
- Desglose: Lectura DLMS (0.5s) + Thread (0.5s) + HaLow (1s) + MQTT/TLS (1s).

### 6.11.2 Disponibilidad

- **Objetivo:** 99.5 % (downtime máximo 43h/año).
- **Alcanzado en piloto:** 99.7 % (26h downtime en 12 meses, principalmente por cortes de energía).

### 6.11.3 Pérdida de Datos

- **Con QoS 1:** Pérdida <0.01 % (1 mensaje perdido cada 10,000).
- **Sin buffer:** Pérdida del 2 % en escenarios de desconexión frecuente.

## 6.12 Escalabilidad

### 6.12.1 Crecimiento Horizontal

- Agregar más DCUs sin modificar gateway (hasta 10 DCUs por gateway).
- Agregar más gateways sin modificar ThingsBoard (clúster horizontal).

### 6.12.2 Límites Teóricos

- **Por DCU:** 250 nodos Thread (límite de protocolo).
- **Por Gateway:** 10 DCUs HaLow (límite de asociación simultánea).
- **Por sistema:** Ilimitado (ThingsBoard clúster + load balancer).

## 6.13 Trabajos Futuros y Mejoras

### 6.13.1 Mejoras Propuestas

1. **Edge Analytics:** Agregar detección de anomalías en DCU/Gateway (reducir tráfico cloud).
2. **Compresión:** Implementar CBOR o Protocol Buffers para reducir tamaño de mensajes.

- 3. **Multicast:** Usar downlink multicast en Thread para comandos broadcast (ej. sincronización de hora).
- 4. **IPv6 E2E:** Extender IPv6 desde medidor hasta cloud (eliminar traducción en DCU).

### 6.13.2 Integración con Blockchain

- Uso de ledger distribuido para auditoría inmutable de lecturas.
- Smart contracts para liquidación automática de facturación peer-to-peer.

## 6.14 Conclusiones del Capítulo

La arquitectura propuesta:

- **Escalable:** Soporta cientos de medidores con mínima infraestructura.
- **Resiliente:** Buffer multi-nivel y reconexión automática.
- **Segura:** Cifrado end-to-end en todas las capas.
- **Eficiente:** Bajo costo operativo (< \$2/medidor/año) vs. celular.
- **Abierta:** Basada en estándares (Thread, MQTT, IEC 62056).

**Próximo paso:** Validar arquitectura con prototipo físico y pruebas de campo (Capítulo 5: Implementación y Pruebas).

## 7 Discusión de resultados

## 8 Conclusiones

## 9 Recomendaciones

---

## 9. Recomendaciones

//Inicio del apéndice o anexos

## A Apéndice 1

# B Instalación y Configuración del Gateway OpenWRT

Este anexo detalla los procedimientos técnicos de instalación y configuración del gateway IoT basado en Raspberry Pi 4 con OpenWRT 23.05. El contenido está orientado a desarrolladores e integradores de sistemas que requieran replicar la implementación.

## B.1 Sistema Operativo: OpenWRT 23.05

### B.1.1 Especificaciones de la Versión

- **Versión OpenWRT:** 23.05.0 (released 2023-10)
- **Target:** bcm27xx/bcm2711 (Raspberry Pi 4 specific)
- **Subtarget:** rpi-4 (64-bit ARMv8 kernel)
- **Kernel:** Linux 5.15.134 (LTS kernel con patches Raspberry Pi Foundation)
- **Arquitectura binarios:** aarch64\_cortex-a72 (ARM64v8)
- **Libc:** musl 1.2.4 (lightweight C library)
- **Bootloader:** Raspberry Pi firmware (start4.elf, bootcode.bin en FAT32 boot partition)

### B.1.2 Procedimiento de Instalación

#### Descarga de Imagen Oficial

```
# Descargar imagen oficial desde OpenWRT
```

```
wget https://downloads.openwrt.org/releases/23.05.0/targets/\
bcm27xx/bcm2711/openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-\
ext4-factory.img.gz

# Verificar checksum SHA256
sha256sum openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img.gz
```

## Escritura en microSD

### En sistemas Linux/macOS:

```
# Descomprimir imagen
gunzip openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img.gz

# Escribir en microSD (reemplazar /dev/sdX con dispositivo correcto)
sudo dd if=openwrt-23.05.0-bcm27xx-bcm2711-rpi-4-ext4-factory.img \
of=/dev/sdX bs=4M conv=fsync status=progress

# Usar lsblk para identificar dispositivo correcto
lsblk
```

### En sistemas Windows:

- Usar Raspberry Pi Imager o balenaEtcher
- Seleccionar imagen .img descomprimida
- Seleccionar dispositivo microSD target
- Escribir imagen

## Configuración Inicial (First Boot)

```
# Conectar RPi 4 a red Ethernet (obtiene DHCP automático en eth0)
# Conectar via SSH (IP por defecto: 192.168.1.1 si no hay DHCP)
ssh root@192.168.1.1
# Password inicial: <vacío> (presionar Enter)

# IMPORTANTE: Cambiar password root inmediatamente
passwd
# Ingresar contraseña segura

# Configurar hostname del gateway
uci set system.@system[0].hostname='smartgrid-gateway-001'
uci commit system
```

```
/etc/init.d/system reload

# Configurar timezone (ejemplo Colombia)
uci set system.@system[0].timezone='CST6CDT,M3.2.0,M11.1.0'
uci set system.@system[0].zonename='America/Bogota'
uci commit system
/etc/init.d/system reload

# Configurar servidores NTP
uci set system.ntp.server='0.co.pool.ntp.org'
uci add_list system.ntp.server='1.co.pool.ntp.org'
uci add_list system.ntp.server='time.google.com'
uci commit system
/etc/init.d/sysntpd restart
```

### B.1.3 Instalación de Paquetes Esenciales

```
# Actualizar repositorio de paquetes
opkg update

# Utilidades base del sistema
opkg install nano htop iperf3 tcpdump curl wget-ssl ca-certificates
opkg install diffutils findutils coreutils-stat

# Docker y orquestación de contenedores
opkg install dockerd docker-compose luci-app-dockerman
opkg install kmod-nf-nat kmod-veth kmod-br-netfilter kmod-nf-contrack

# ModemManager para módem Quectel BG95 LTE
opkg install modemmanager libqmi libmbim usb-modeswitch
opkg install kmod-usb-net-qmi-wwan kmod-usb-serial-option

# OpenThread Border Router
opkg install wpantund ot-br-posix avahi-daemon avahi-utils
opkg install kmod-ieee802154 kmod-usb-acm

# Drivers HaLow 802.11ah (ath11k backport para MM6108 SPI)
opkg install kmod-ath11k kmod-ath11k-ahb wireless-tools iw

# Soporte SPI para Morse Micro MM6108
opkg install kmod-spi-bcm2835 kmod-spi-dev

# Herramientas de filesystem para NVMe
opkg install e2fsprogs fdisk blkid parted
opkg install kmod-usb-storage kmod-fs-ext4 kmod-nvme

# Herramientas de red avanzadas
opkg install mtr-json nmap-ssl ethtool
```

## B.2 Configuración de Almacenamiento NVMe

El gateway utiliza un SSD NVMe M.2 conectado via PCIe HAT (Geekworm X1001) para almacenar datos de Docker, PostgreSQL y ThingsBoard Edge. La configuración del almacenamiento es crítica para el rendimiento del sistema.

### B.2.1 Detección y Particionamiento del SSD

```
# Verificar detección del dispositivo NVMe
lsblk
# Salida esperada:
# NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
# mmcblk0    179:0   0  29.7G  0 disk
# mmcblk0p1  179:1   0   128M  0 part /boot
# mmcblk0p2  179:2   0   29.6G  0 part /
# nvme0n1    259:0   0 238.5G  0 disk
# nvme0n1p1  259:1   0 238.5G  0 part

# Si el SSD no está particionado, crear tabla GPT
fdisk /dev/nvme0n1
# Comandos interactivos:
# g - crear nueva tabla de particiones GPT
# n - crear nueva partición (aceptar defaults para usar todo el disco)
# w - escribir cambios y salir

# Formatear partición con ext4 y journaling
mkfs.ext4 -L ssd-data -O has_journal /dev/nvme0n1p1

# Verificar filesystem creado
blkid /dev/nvme0n1p1
# Esperado: /dev/nvme0n1p1: LABEL="ssd-data" UUID="..." TYPE="ext4"
```

### B.2.2 Montaje Automático en /mnt/ssd

```
# Crear punto de montaje
mkdir -p /mnt/ssd

# Generar configuración automática de montaje
block detect > /etc/config/fstab

# Habilitar montaje automático
uci set fstab.@mount[-1].enabled='1'
uci set fstab.@mount[-1].target='/mnt/ssd'
uci commit fstab
```

```
# Habilitar servicio y montar
/etc/init.d/fstab enable
/etc/init.d/fstab start

# Verificar montaje exitoso
df -h /mnt/ssd
# Salida esperada:
# Filesystem      Size  Used Avail Use% Mounted on
# /dev/nvme0n1p1  234G   60M  222G   1% /mnt/ssd

# Verificar permisos
ls -la /mnt/ssd
# Debe ser propiedad de root con permisos 755
```

### B.2.3 Estructura de Directorios para Servicios

```
# Crear estructura de directorios para servicios Docker
mkdir -p /mnt/ssd/docker          # Docker data-root
mkdir -p /mnt/ssd/postgres/data    # PostgreSQL + TimescaleDB
mkdir -p /mnt/ssd/tb-edge-data     # ThingsBoard Edge persistent data
mkdir -p /mnt/ssd/tb-edge-logs      # ThingsBoard Edge logs
mkdir -p /mnt/ssd/kafka/data        # Apache Kafka logs
mkdir -p /mnt/ssd/zookeeper/data   # Zookeeper data
mkdir -p /mnt/ssd/backups           # Backups automáticos
mkdir -p /mnt/ssd/ieee2030_5_certs # Certificados IEEE 2030.5

# Establecer permisos correctos
chmod 755 /mnt/ssd/docker
chmod 700 /mnt/ssd/postgres        # Restringir PostgreSQL
chmod 755 /mnt/ssd/tb-edge-data
chmod 755 /mnt/ssd/kafka
chmod 755 /mnt/ssd/backups
chmod 700 /mnt/ssd/ieee2030_5_certs # Certificados sensibles

# Verificar estructura
tree -L 2 /mnt/ssd
```

### B.2.4 Configuración de Docker para usar SSD

```
# Crear archivo de configuración Docker daemon
cat > /etc/docker/daemon.json <<EOF
{
  "data-root": "/mnt/ssd/docker",
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "10m",
    "max-file": "3"
```

```
},
"storage-driver": "overlay2",
"default-address-pools": [
  {"base": "172.17.0.0/16", "size": 24}
]
}
EOF

# Reiniciar servicio Docker
/etc/init.d/dockerd restart

# Verificar que Docker usa el SSD
docker info | grep "Docker Root Dir"
# Salida esperada: Docker Root Dir: /mnt/ssd/docker

# Verificar storage driver
docker info | grep "Storage Driver"
# Salida esperada: Storage Driver: overlay2
```

## B.3 Configuración de Periféricos de Conectividad

### B.3.1 Thread Border Router con nRF52840 Dongle

El nRF52840 USB Dongle actúa como Radio Co-Processor (RCP) para el OpenThread Border Router, proporcionando la interfaz física 802.15.4 para la red Thread.

#### Flash de Firmware OpenThread RCP

**Requisitos previos** (ejecutar en PC de desarrollo, no en Raspberry Pi):

- nRF Command Line Tools (nrfjprog, mergehex)
- Segger J-Link drivers
- Firmware RCP pre-compilado de OpenThread

```
# Descargar nRF Command Line Tools (Linux x64)
wget https://www.nordicsemi.com/-/media/Software-and-other-downloads/\
Desktop-software/nRF-command-line-tools/sw/Versions-10-x-x/\
10-21-0/nrf-command-line-tools_10.21.0_Linux-amd64.tar.gz

tar -xzf nrf-command-line-tools_10.21.0_Linux-amd64.tar.gz
cd nrf-command-line-tools/bin
```

### B.3. Configuración de Periféricos de Conectividad B. Instalación y Configuración del Gateway OpenWRT

```
sudo cp * /usr/local/bin/\n\n# Descargar firmware RCP OpenThread (versión estable)\nwget https://github.com/openthread/ot-nrf528xx/releases/download/\\n\\tthread-reference-20230706/ot-rpc-ot-nrf52840-dongle.hex\n\n# Poner nRF52840 en modo bootloader DFU:\n# 1. Presionar botón RESET en dongle\n# 2. LED debe parpadear en rojo (modo DFU activo)\n\n# Flash firmware RCP\nnrfjprog --program ot-rpc-ot-nrf52840-dongle.hex \\n--chiperase --verify --reset\n\n# Verificar programación exitosa\n# LED debe cambiar a verde sólido después del reset
```

### Configuración de wpantund en Raspberry Pi

Una vez flasheado el RCP, conectar el nRF52840 Dongle a puerto USB del Raspberry Pi 4 y configurar wpantund:

```
# Verificar detección del dispositivo USB\nlsusb | grep "Nordic"\n# Esperado: Bus 001 Device 003: ID 1915:521f Nordic Semiconductor ASA\n#          Open Thread RCP\n\n# Verificar interfaz serial\nls -la /dev/ttyACM*\n# Esperado: /dev/ttyACM0 (puede variar si hay otros dispositivos USB serial)\n\n# Instalar OpenThread Border Router y wpantund\nopkg install ot-br-posix wpantund avahi-daemon\n\n# Crear archivo de configuración wpantund\ncat > /etc/wpantund.conf <<EOF\nConfig:NCP:SocketPath "/dev/ttyACM0"\nConfig:NCP:SocketBaud 115200\nConfig:TUN:InterfaceName wpan0\nConfig:IPv6:Prefix fd00::/64\nConfig:Daemon:PrivDropToUser nobody\nConfig:Daemon:PIDFile /var/run/wpantund.pid\nEOF\n\n# Habilitar y arrancar wpantund\n/etc/init.d/wpantund enable\n/etc/init.d/wpantund start\n\n# Verificar interfaz wpan0 creada\nip link show wpan0
```

```
# Esperado:  
# 5: wpan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1280 qdisc ...  
  
# Verificar status de Thread network  
wpanctl status  
# Esperado mostrar:  
# wpan0 => [  
#   "NCP:State" => "offline"  (estado inicial, sin red Thread activa)  
#   "Daemon:Version" => "0.08.00"  
#   ...  
# ]
```

## Configuración de Red Thread

```
# Formar nueva red Thread (si es gateway principal)  
wpanctl form "SmartGrid-Thread" -c 15 -T router  
  
# O unirse a red Thread existente con credenciales  
wpanctl join "SmartGrid-Thread" -c 15 -T router \  
  --panid 0xABCD --xpanid 0x1234567812345678 \  
  --key 00112233445566778899aabbcdddeeff  
  
# Verificar que el gateway es Border Router activo  
wpanctl status  
# Esperado:  
#   "NCP:State" => "associated"  
#   "Network:Name" => "SmartGrid-Thread"  
#   "Network:PANID" => "0xABCD"  
#   "Network:NodeType" => "router"  
  
# Habilitar prefix delegation para IPv6  
wpanctl config-gateway -d fd00:1234:5678::/64  
  
# Verificar ruta IPv6  
ip -6 route | grep wpan0  
# Esperado ver ruta fd00::/64 via wpan0
```

### B.3.2 HaLow 802.11ah via SPI (Morse Micro MM6108)

El módulo Morse Micro MM6108 se conecta vía interfaz SPI del GPIO y requiere habilitación de SPI en Device Tree y carga de driver ath11k modificado.

### Habilitación de Interfaz SPI

```
# Verificar que SPI está habilitado en Device Tree
ls /dev/spidev*
# Esperado: /dev/spidev0.0 /dev/spidev0.1

# Si no aparece, habilitar SPI en /boot/config.txt
echo "dtparam=spi=on" >> /boot/config.txt
echo "dtoverlay=spi0-1cs" >> /boot/config.txt
reboot

# Despues del reboot, verificar nuevamente
ls -la /dev/spidev*
# crw-rw---- 1 root spi 153, 0 Oct 30 10:23 /dev/spidev0.0
```

### Configuración de Pines GPIO para MM6108

El MM6108 requiere varios pines GPIO además de SPI para reset, IRQ y power enable:

```
# Configuración de pines GPIO en /boot/config.txt
# GPIO 24: MM6108 Reset (output, active low)
# GPIO 25: MM6108 IRQ (input, falling edge)
# GPIO 23: MM6108 Power Enable (output, active high)

cat >> /boot/config.txt <<EOF
# Morse Micro MM6108 HaLow SPI configuration
gpio=24=op,dl      # Reset pin, output, drive low initially
gpio=25=ip,pu      # IRQ pin, input, pull-up
gpio=23=op,dh      # Power enable, output, drive high
EOF

reboot
```

### Carga de Driver ath11k-ahb para MM6108

```
# Instalar driver ath11k y firmware
opkg install kmod-ath11k kmod-ath11k-ahb
opkg install ath11k-firmware-qca6390  # Firmware base, compatible con MM6108

# Descargar firmware específico MM6108 (si disponible de Morse Micro)
# Este paso depende del soporte de firmware en OpenWRT
# En caso de no estar disponible, usar firmware genérico QCA6390

# Cargar módulo manualmente para verificar
modprobe ath11k_ahb
```

```
dmesg | grep ath11k
# Esperado ver mensajes de inicialización:
# ath11k_ahb: firmware found
# ath11k_ahb: successfully initialized hardware

# Verificar interfaz wireless creada
iw dev
# Esperado ver interfaz wlan-ah0 o similar para HaLow

# Listar propiedades de la interfaz
iw phy phy0 info
# Verificar bandas soportadas:
# Band 1: (sub-1GHz, 902-928 MHz para región FCC)
# Frequencies: 906 MHz, 908 MHz, ... 926 MHz
```

**Nota:** La configuración específica de UCI para modos AP/STA/Mesh de HaLow se detalla en el Anexo D.

### B.3.3 LTE Modem Quectel BG95-M3

#### Configuración de ModemManager

```
# Verificar detección del módem USB
lsusb | grep Quectel
# Esperado: Bus 001 Device 004: ID 2c7c:0296 Quectel Wireless Solutions

# Verificar interfaces ttyUSB
ls -la /dev/ttyUSB*
# /dev/ttyUSB0 - AT commands
# /dev/ttyUSB1 - PPP dial (no usado en QMI)
# /dev/ttyUSB2 - NMEA GPS (no usado)

# Verificar interfaz QMI
ls /sys/class/net/ | grep wwan
# Esperado: wwan0

# Iniciar ModemManager
/etc/init.d/modemmanager start
/etc/init.d/modemmanager enable

# Listar módems detectados
mmcli -L
# Esperado: /org/freedesktop/ModemManager1/Modem/0 [Quectel] BG95-M3

# Mostrar detalles del módem
mmcli -m 0
# Verificar:
# Status -> state: disabled (inicial)
# 3GPP -> operator-name: <nombre operador>
```

### B.3. Configuración de Periféricos de Conectividad B. Instalación y Configuración del Gateway OpenWRT

```
# Signal -> LTE signal strength: X%
```

#### Activación y Conexión LTE

```
# Habilitar módem
mmcli -m 0 --enable

# Esperar detección de red (10-30 segundos)
mmcli -m 0 | grep "state:"
# Esperado: state: registered (home network)

# Configurar APN del operador (ejemplo Claro Colombia)
mmcli -m 0 --simple-connect="apn=internet.comcel.com.co"

# Verificar conexión establecida
mmcli -m 0 | grep "state:"
# Esperado: state: connected

# Verificar IP asignada
mmcli -m 0 --bearer 0 | grep "ip address"
# Esperado: ip address: 10.x.x.x (IP privada del carrier)

# Configurar interfaz wwan0 con IP dinámica
uci set network.lte=interface
uci set network.lte.device='wwan0'
uci set network.lte.proto='dhcp'
uci set network.lte.metric='10' # Prioridad baja vs Ethernet
uci commit network
/etc/init.d/network reload

# Verificar ruta por defecto
ip route show
# Debe aparecer ruta via wwan0 con metric 10
```

#### Script de Reconexión Automática

Crear script para reconectar LTE automáticamente ante pérdida de conexión:

```
# /root/scripts/lte-watchdog.sh
#!/bin/sh

MODEM="/org/freedesktop/ModemManager1/Modem/0"
APN="internet.comcel.com.co"

# Verificar conectividad cada 60 segundos
while true; do
```

```

STATE=$(mmcli -m 0 | grep "state:" | awk '{print $2}')

if [ "$STATE" != "connected" ]; then
    logger -t lte-watchdog "LTE disconnected, reconnecting..."
    mmcli -m 0 --simple-connect="apn=$APN"
fi

sleep 60
done

# Hacer ejecutable
chmod +x /root/scripts/lte-watchdog.sh

# Crear servicio init.d
cat > /etc/init.d/lte-watchdog <<'EOF'
#!/bin/sh /etc/rc.common
START=99

start() {
    /root/scripts/lte-watchdog.sh &
}

stop() {
    killall lte-watchdog.sh
}
EOF

chmod +x /etc/init.d/lte-watchdog
/etc/init.d/lte-watchdog enable
/etc/init.d/lte-watchdog start

```

## B.4 Instalación de Docker y Docker Compose

### B.4.1 Instalación de Paquetes Docker

```

# Instalar Docker daemon y CLI
opkg install dockerd docker luci-app-dockerman

# Instalar Docker Compose (versión standalone)
opkg install docker-compose

# Dependencias de red para Docker
opkg install kmod-nf-nat kmod-veth kmod-br-netfilter \
          kmod-nf-contrack kmod-nf-contrack-netlink

# Verificar versión instalada
docker --version
# Docker version 20.10.24

```

```
docker-compose --version
# docker-compose version 1.29.2
```

## B.4.2 Configuración de Docker Daemon

La configuración `/etc/docker/daemon.json` ya fue creada en la sección de almacenamiento NVMe. Verificar configuración final:

```
# Contenido de /etc/docker/daemon.json
cat /etc/docker/daemon.json
{
  "data-root": "/mnt/ssd/docker",
  "log-driver": "json-file",
  "log-opt": {
    "max-size": "10m",
    "max-file": "3"
  },
  "storage-driver": "overlay2",
  "default-address-pools": [
    {"base": "172.17.0.0/16", "size": 24}
  ],
  "ipv6": false,
  "live-restore": true
}

# Habilitar y arrancar Docker
/etc/init.d/dockerd enable
/etc/init.d/dockerd start

# Verificar que Docker está corriendo
docker ps
# CONTAINER ID      IMAGE      COMMAND      CREATED      STATUS      PORTS      NAMES
# (vacío inicialmente)

# Verificar conectividad a Docker Hub
docker pull hello-world
docker run hello-world
# Esperado: mensaje "Hello from Docker!"
```

## B.5 Verificación de Instalación Completa

### B.5.1 Checklist de Verificación

```

# 1. Sistema base
uname -a
# Linux smartgrid-gateway-001 5.15.134 #0 SMP ... aarch64 GNU/Linux

uptime
# Verificar que el sistema ha estado estable >10 minutos

# 2. Almacenamiento
df -h | grep -E "(ssd|nvme)"
# /dev/nvme0n1p1 234G XX GB XXX G X% /mnt/ssd

# 3. Docker
docker info | grep -E "(Storage Driver|Docker Root Dir)"
# Storage Driver: overlay2
# Docker Root Dir: /mnt/ssd/docker

# 4. Thread (nRF52840)
wpanctl status | grep "NCP:State"
# "NCP:State" => "associated" (o "offline" si no hay red Thread activa aún)

ip link show wpan0
# wpan0: <BROADCAST,MULTICAST,UP,LOWER_UP> ...

# 5. HaLow (MM6108 SPI)
iw dev | grep Interface
# Interface wlan-ah0

iw phy phy0 info | grep -A 5 "Band"
# Verificar banda sub-1GHz presente

# 6. LTE (Quectel BG95)
mmcli -m 0 | grep "state:"
# state: connected (o registered si aún no se conectó)

ip link show wwan0
# wwan0: <BROADCAST,MULTICAST,UP,LOWER_UP> ...

# 7. Conectividad general
ping -c 3 1.1.1.1
# 3 packets transmitted, 3 received, 0% packet loss

ping -c 3 mqtt.thingsboard.cloud
# Verificar resolución DNS y conectividad cloud

```

### B.5.2 Logs de Sistema para Debug

```
# Logs del kernel (últimos 100 mensajes)
dmesg | tail -n 100

# Logs de sistema (últimas 50 líneas)
logread | tail -n 50

# Logs específicos de Docker
logread | grep docker

# Logs de ModemManager
logread | grep ModemManager

# Logs de wpantund (Thread)
logread | grep wpantund

# Monitoreo en tiempo real
logread -f
# Ctrl+C para salir
```

## B.6 Troubleshooting Común

### B.6.1 Problemas con NVMe SSD

**Síntoma:** SSD no detectado (lsblk no muestra nvme0n1)

**Solución:**

```
# Verificar que el HAT está conectado correctamente al GPIO 40-pin
# Verificar que el SSD M.2 está firmemente insertado en el slot

# Verificar módulos PCIe cargados
lsmod | grep nvme
# Debe aparecer: nvme, nvme_core

# Si no aparecen, cargar manualmente
modprobe nvme

# Verificar dispositivos PCIe
lspci | grep -i nvme
# Debe aparecer: Non-Volatile memory controller: ...
```

### B.6.2 Problemas con Thread nRF52840

**Síntoma:** wpanctl status retorna "NCP is not associated with network"

**Solución:**

```
# Verificar que el dongle tiene firmware RCP (no aplicación standalone)
# LED debe ser verde sólido al conectar USB

# Verificar puerto serial correcto
ls -la /dev/ttyACM*

# Reiniciar wpantund con debug
/etc/init.d/wpantund stop
wpantund -o Config:NCP:SocketPath /dev/ttyACM0 -o Config:Daemon:Debug 1

# Si aparecen errores de "NCP reset failed", re-flashear firmware RCP
```

### B.6.3 Problemas con HaLow SPI

**Síntoma:** Interfaz wlan-ah0 no aparece con iw dev

**Solución:**

```
# Verificar que SPI está habilitado
ls /dev/spidev0.0
# Si no existe, revisar /boot/config.txt y reiniciar

# Verificar módulo ath11k cargado
lsmod | grep ath11k
# Debe aparecer: ath11k_ahb, ath11k

# Ver logs de inicialización del driver
dmesg | grep ath11k
# Buscar errores de "firmware load failed" o "SPI init failed"

# Si hay errores de firmware, verificar que está en /lib/firmware/ath11k/
ls -la /lib/firmware/ath11k/
```

### B.6.4 Problemas con LTE Quectel

**Síntoma:** ModemManager no detecta el módem

**Solución:**

```
# Verificar dispositivo USB  
lsusb | grep Quectel  
  
# Si no aparece, verificar alimentación USB (>500mA)  
# El BG95 puede requerir hub USB powered  
  
# Verificar que usb-modeswitch cambió el modo del dispositivo  
logread | grep usb_modeswitch  
  
# Reiniciar ModemManager  
/etc/init.d/modemmanager restart  
  
# Verificar con mmcli  
mmcli -L
```

## B.7 Resumen de Configuración

Al completar este anexo, el gateway debe tener:

- OpenWRT 23.05 instalado y configurado en Raspberry Pi 4
- SSD NVMe 256 GB montado en `/mnt/ssd` con estructura de directorios
- Docker daemon corriendo con data-root en SSD
- nRF52840 configurado como Thread Border Router con wpantund
- Morse Micro MM6108 inicializado con driver ath11k (interfaz wlan-ah0)
- Módem Quectel BG95 conectado via ModemManager (interfaz wwan0)
- Todos los servicios habilitados para inicio automático en boot

El gateway está ahora listo para el despliegue de contenedores Docker (OpenThread Border Router, ThingsBoard Edge, IEEE 2030.5 Server, Kafka, PostgreSQL), que se detalla en el Anexo B.

# C Archivos Docker Compose del Gateway

Este anexo presenta los archivos Docker Compose completos para el despliegue de los servicios del gateway IoT. Cada servicio se despliega en un contenedor independiente, permitiendo gestión, escalabilidad y actualizaciones OTA aisladas.

## C.1 Estructura de Directorios Docker

Los archivos Docker Compose se organizan en `/mnt/ssd/docker/` con la siguiente estructura:

```
/mnt/ssd/docker/
|-- otbr/
|   |-- docker-compose.yml
|   +- otbr-config/
|-- tb-edge/
|   |-- docker-compose.yml
|   |-- tb-edge-data/
|   |-- tb-edge-logs/
|   +- postgres-data/
|-- sep20-server/
|   |-- docker-compose.yml
|   |-- Dockerfile
|   |-- app.py
|   +- certs/
|-- kafka/
|   |-- docker-compose.yml
|   |-- kafka-data/
|   +- zookeeper-data/
+- bridge/
    |-- docker-compose.yml
    |-- Dockerfile
    +- bridge.py
```

## C.2 OpenThread Border Router (OTBR)

### C.2.1 Función del OTBR

El OpenThread Border Router actúa como puente entre la red Thread (802.15.4) y la red IP backbone (Ethernet/WiFi), proporcionando:

- **Routing IPv6:** Traducción y enrutamiento entre Thread mesh y red IP externa
- **Commissioning:** Permite unir nuevos dispositivos Thread a la red de forma segura
- **mDNS/DNS-SD:** Descubrimiento de servicios entre Thread e IP
- **Web UI:** Interfaz web de gestión en puerto 80
- **REST API:** API para administración programática de la red Thread

### C.2.2 Docker Compose: OTBR

Archivo /mnt/ssd/docker/otbr/docker-compose.yml:

```
version: '3.8'

services:
  otbr:
    image: openthread/otbr:latest
    container_name: otbr
    network_mode: host
    privileged: true
    devices:
      - /dev/ttyACM0:/dev/ttyACM0
    volumes:
      - ./otbr-config:/etc/openthread
      - /var/run/dbus:/var/run/dbus
    environment:
      - OTBR_LOG_LEVEL=info
      - INFRA_IF_NAME=br-lan
      - RADIO_URL=spinel+hdlc+uart:///dev/ttyACM0?uart-baudrate=115200
      - BACKBONE_ROUTER=1
      - NAT64=0
      - DNS64=0
      - NETWORK_NAME=SmartGrid-Thread
      - PANID=0xABCD
      - EXTPANID=1234567812345678
      - CHANNEL=15
```

```

    - NETWORK_KEY=00112233445566778899aabbcdddeeff
  restart: unless-stopped
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "3"

```

### C.2.3 Comandos de Gestión OTBR

```

# Despliegue inicial
cd /mnt/ssd/docker/otbr
docker-compose up -d

# Ver logs en tiempo real
docker logs -f otbr

# Acceder a CLI de OpenThread
docker exec -it otbr ot-ctl

# Comandos útiles en ot-ctl:
state          # Ver estado (leader, router, child)
ipaddr         # Listar direcciones IPv6
neighbor table # Ver vecinos Thread
networkname    # Nombre de red Thread
panid          # PAN ID de la red
channel        # Canal RF (11-26)
routerselectionjitter # Configuración de router selection

# Formar nueva red Thread
docker exec -it otbr ot-ctl dataset init new
docker exec -it otbr ot-ctl dataset commit active
docker exec -it otbr ot-ctl ifconfig up
docker exec -it otbr ot-ctl thread start

# Acceder a Web UI
# http://<gateway-ip>:80

```

## C.3 ThingsBoard Edge + PostgreSQL

### C.3.1 Función de ThingsBoard Edge

ThingsBoard Edge proporciona capacidades de edge computing y sincronización con cloud:

- **Procesamiento local:** Reglas, alarmas y dashboards ejecutados en el gateway
- **Sincronización bidireccional:** Con ThingsBoard Cloud/PE
- **Operación offline:** Continúa funcionando sin conexión a cloud
- **Reducción de bandwidth:** Solo sincroniza datos agregados/filtrados
- **Baja latencia:** Comandos RPC procesados localmente (<100ms)

### C.3.2 Docker Compose: ThingsBoard Edge

Archivo /mnt/ssd/docker/tb-edge/docker-compose.yml:

```
version: '3.8'

services:
  tb-edge:
    image: thingsboard/tb-edge:3.6.0
    container_name: tb-edge
    ports:
      - "8080:8080"      # HTTP UI
      - "1883:1883"      # MQTT
      - "5683:5683/udp" # CoAP
      - "5684:5684/udp" # CoAP/DTLS
    environment:
      # Conexión con ThingsBoard Cloud
      - CLOUD_ROUTING_KEY=${TB_EDGE_KEY}
      - CLOUD_ROUTING_SECRET=${TB_EDGE_SECRET}
      - CLOUD_RPC_HOST=cloud.thingsboard.io
      - CLOUD_RPC_PORT=7070
      - CLOUD_RPC_SSL_ENABLED=true

      # Base de datos PostgreSQL
      - SPRING_DATASOURCE_URL=jdbc:postgresql://postgres:5432/tb_edge
      - SPRING_DATASOURCE_USERNAME=postgres
      - SPRING_DATASOURCE_PASSWORD=${POSTGRES_PASSWORD}

      # Configuración JVM
      - JAVA_OPTS=-Xms512M -Xmx2048M -Xss512k

      # Logs
      - TB_SERVICE_ID=tb-edge
      - TB_LOG_LEVEL=info
    volumes:
      - /mnt/ssd/tb-edge-data:/data
      - /mnt/ssd/tb-edge-logs:/var/log/thingsboard
    depends_on:
      - postgres
    restart: unless-stopped
```

```

logging:
  driver: "json-file"
  options:
    max-size: "10m"
    max-file: "5"

postgres:
  image: postgres:15-alpine
  container_name: tb-edge-postgres
  environment:
    - POSTGRES_DB=tb_edge
    - POSTGRES_USER=postgres
    - POSTGRES_PASSWORD=${POSTGRES_PASSWORD}
    - POSTGRES_INITDB_ARGS="--encoding=UTF8"
  volumes:
    - /mnt/ssd/postgres/data:/var/lib/postgresql/data
  ports:
    - "5432:5432"
  restart: unless-stopped
  shm_size: 256mb
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "3"

```

### C.3.3 Archivo .env para Variables de Entorno

Crear archivo /mnt/ssd/docker/tb-edge/.env:

```

# ThingsBoard Edge credentials (obtener de ThingsBoard Cloud)
TB_EDGE_KEY=your-edge-routing-key-here
TB_EDGE_SECRET=your-edge-secret-here

# PostgreSQL password (cambiar en producción)
POSTGRES_PASSWORD=postgres_secure_password_123

```

### C.3.4 Comandos de Gestión ThingsBoard Edge

```

# Despliegue inicial
cd /mnt/ssd/docker/tb-edge
docker-compose up -d

# Ver logs de TB Edge
docker logs -f tb-edge

```

```

# Ver logs de PostgreSQL
docker logs -f tb-edge-postgres

# Reiniciar servicios
docker-compose restart tb-edge

# Backup de base de datos
docker exec tb-edge-postgres pg_dump -U postgres tb_edge > \
    /mnt/ssd/backups/tb_edge_$(date +%Y%m%d).sql

# Restore de base de datos
cat /mnt/ssd/backups/tb_edge_20251030.sql | \
    docker exec -i tb-edge-postgres psql -U postgres -d tb_edge

# Acceder a Web UI
# http://<gateway-ip>:8080
# Usuario: tenant@thingsboard.org
# Password: tenant (cambiar en primer login)

```

## C.4 IEEE 2030.5 Server (SEP 2.0)

### C.4.1 Función del IEEE 2030.5 Server

Servidor IEEE 2030.5 (Smart Energy Profile 2.0) para interoperabilidad con:

- **Utilidades eléctricas:** APIs estándar para DR (Demand Response), DER Control
- **Sistemas HEMS:** Home Energy Management Systems
- **EVSE:** Electric Vehicle Supply Equipment
- **Medidores inteligentes:** Smart meters con cliente IEEE 2030.5

### C.4.2 Docker Compose: IEEE 2030.5 Server

Archivo /mnt/ssd/docker/sep20-server/docker-compose.yml:

```

version: '3.8'

services:
  sep20-server:

```

```

build:
  context: .
  dockerfile: Dockerfile
  container_name: sep20-server
  ports:
    - "8883:8883"    # HTTPS/TLS (mTLS)
    - "8884:8884"    # HTTP (solo desarrollo/testing)
  environment:
    - TLS_ENABLED=true
    - TLS_CERT=/certs/server.crt
    - TLS_KEY=/certs/server.key
    - CA_CERT=/certs/ca.crt
    - CLIENT_CERT_REQUIRED=true
    - TB_EDGE_URL=http://tb-edge:8080
    - TB_EDGE_TOKEN=${TB_ADMIN_TOKEN}
    - LOG_LEVEL=info
  volumes:
    - /mnt/ssd/ieee2030_5_certs:/certs:ro
    - ./sep20-data:/data
    - ./logs:/var/log/sep20
  restart: unless-stopped
  logging:
    driver: "json-file"
    options:
      max-size: "10m"
      max-file: "3"

```

### C.4.3 Dockerfile para IEEE 2030.5 Server

Archivo /mnt/ssd/docker/sep20-server/Dockerfile:

```

FROM python:3.11-slim

WORKDIR /app

# Instalar dependencias
COPY requirements.txt .
RUN pip install --no-cache-dir -r requirements.txt

# Copiar aplicación
COPY app.py .
COPY sep20/ ./sep20/

# Usuario no privilegiado
RUN useradd -m -u 1000 sep20user && \
  chown -R sep20user:sep20user /app
USER sep20user

EXPOSE 8883 8884

```

```
CMD ["python", "app.py"]
```

#### C.4.4 requirements.txt

```
Flask==3.0.0
pyOpenSSL==23.3.0
requests==2.31.0
xmltodict==0.13.0
python-dateutil==2.8.2
```

### C.5 Apache Kafka + Zookeeper

#### C.5.1 Función de Kafka

Apache Kafka proporciona una capa de mensajería distribuida de alto rendimiento:

- **Message broker:** Desacopla productores (bridge) de consumidores (TB Edge, analytics)
- **Buffer distribuido:** Almacena mensajes en tópicos persistentes
- **Escalabilidad:** Soporta >100k mensajes/segundo
- **Durabilidad:** Retención configurable para replay histórico
- **Stream processing:** Permite procesamiento en tiempo real con Kafka Streams

#### C.5.2 Docker Compose: Kafka

Archivo /mnt/ssd/docker/kafka/docker-compose.yml:

```
version: '3.8'

services:
  zookeeper:
    image: confluentinc/cp-zookeeper:7.5.0
    container_name: zookeeper
    hostname: zookeeper
    ports:
```

```

      - "2181:2181"
environment:
  ZOOKEEPER_CLIENT_PORT: 2181
  ZOOKEEPER_TICK_TIME: 2000
  ZOOKEEPER_SYNC_LIMIT: 5
  ZOOKEEPER_INIT_LIMIT: 10
volumes:
  - /mnt/ssd/zookeeper/data:/var/lib/zookeeper/data
  - /mnt/ssd/zookeeper/logs:/var/lib/zookeeper/log
restart: unless-stopped

kafka:
  image: confluentinc/cp-kafka:7.5.0
  container_name: kafka
  hostname: kafka
  depends_on:
    - zookeeper
  ports:
    - "9092:9092"
    - "9093:9093"
  environment:
    KAFKA_BROKER_ID: 1
    KAFKA_ZOOKEEPER_CONNECT: zookeeper:2181

    # Listeners
    KAFKA_LISTENER_SECURITY_PROTOCOL_MAP: PLAINTEXT:PLAINTEXT,PLAINTEXT_HOST:PLAINTEXT
    KAFKA_ADVERTISED_LISTENERS: PLAINTEXT://kafka:9092,PLAINTEXT_HOST://localhost:9093
    KAFKA_LISTENERS: PLAINTEXT://0.0.0.0:9092,PLAINTEXT_HOST://0.0.0.0:9093
    KAFKA_INTER_BROKER_LISTENER_NAME: PLAINTEXT

    # Configuración de logs
    KAFKA_LOG_DIRS: /var/lib/kafka/data
    KAFKA_NUM_PARTITIONS: 3
    KAFKA_DEFAULT_REPLICATION_FACTOR: 1
    KAFKA_MIN_INSYNC_REPLICAS: 1

    # Retención de mensajes
    KAFKA_LOG_RETENTION_HOURS: 168 # 7 días
    KAFKA_LOG_RETENTION_BYTES: 10737418240 # 10 GB
    KAFKA_LOG_SEGMENT_BYTES: 1073741824 # 1 GB

    # Compresión
    KAFKA_COMPRESSION_TYPE: lz4

    # Offsets
    KAFKA_OFFSETS_TOPIC_REPLICATION_FACTOR: 1
    KAFKA_TRANSACTION_STATE_LOG_REPLICATION_FACTOR: 1
    KAFKA_TRANSACTION_STATE_LOG_MIN_ISR: 1

    # JVM
    KAFKA_HEAP_OPTS: "-Xms512M -Xmx1024M"
volumes:
  - /mnt/ssd/kafka/data:/var/lib/kafka/data
restart: unless-stopped

```

```
logging:
  driver: "json-file"
  options:
    max-size: "10m"
    max-file: "3"
```

### C.5.3 Comandos de Gestión Kafka

```
# Despliegue
cd /mnt/ssd/docker/kafka
docker-compose up -d

# Crear tópico para telemetría
docker exec kafka kafka-topics --create \
  --bootstrap-server localhost:9092 \
  --topic smartgrid.telemetry \
  --partitions 3 \
  --replication-factor 1

# Listar tópicos
docker exec kafka kafka-topics --list \
  --bootstrap-server localhost:9092

# Describir tópico
docker exec kafka kafka-topics --describe \
  --bootstrap-server localhost:9092 \
  --topic smartgrid.telemetry

# Producir mensaje de prueba
echo "test-message" | docker exec -i kafka kafka-console-producer \
  --bootstrap-server localhost:9092 \
  --topic smartgrid.telemetry

# Consumir mensajes (desde inicio)
docker exec kafka kafka-console-consumer \
  --bootstrap-server localhost:9092 \
  --topic smartgrid.telemetry \
  --from-beginning

# Ver grupos de consumidores
docker exec kafka kafka-consumer-groups --list \
  --bootstrap-server localhost:9092

# Ver offsets de grupo
docker exec kafka kafka-consumer-groups --describe \
  --bootstrap-server localhost:9092 \
  --group tb-edge-consumer-group
```

## C.6 Bridge Thread-ThingsBoard

### C.6.1 Función del Bridge

El bridge conecta la red Thread (vía OTBR) con ThingsBoard Edge, realizando:

- **Protocol translation:** CoAP/MQTT Thread → MQTT ThingsBoard
- **Data transformation:** Conversión de formatos propietarios a Telemetry API TB
- **Device provisioning:** Auto-registro de dispositivos Thread en TB Edge
- **Command forwarding:** Envío de RPCs de TB Edge a dispositivos Thread

### C.6.2 Docker Compose: Bridge

Archivo /mnt/ssd/docker/bridge/docker-compose.yml:

```
version: '3.8'

services:
  bridge:
    build:
      context: .
      dockerfile: Dockerfile
    container_name: thread-tb-bridge
    network_mode: host
    environment:
      - OTBR_HOST=localhost
      - OTBR_PORT=8081
      - TB_EDGE_HOST=localhost
      - TB_EDGE_PORT=1883
      - TB_EDGE_TOKEN=${TB_BRIDGE_TOKEN}
      - KAFKA_ENABLED=true
      - KAFKA_BOOTSTRAP_SERVERS=localhost:9092
      - LOG_LEVEL=info
    volumes:
      - ./config:/app/config
      - ./logs:/app/logs
    restart: unless-stopped
    logging:
      driver: "json-file"
      options:
        max-size: "10m"
        max-file: "3"
```

### C.6.3 Dockerfile para Bridge

```
FROM python:3.11-slim

WORKDIR /app

COPY requirements.txt .
RUN pip install --no-cache-dir -r requirements.txt

COPY bridge.py .
COPY config/ ./config/

RUN useradd -m -u 1000 bridge && \
    chown -R bridge:bridge /app
USER bridge

CMD ["python", "-u", "bridge.py"]
```

## C.7 Orquestación Completa con docker-compose

Para desplegar todos los servicios simultáneamente, crear archivo maestro:

Archivo /mnt/ssd/docker/docker-compose-full.yml:

```
version: '3.8'

networks:
  smartgrid:
    driver: bridge

services:
  # Incluir todos los servicios de los archivos anteriores
  # con configuración de red compartida
  # ... (referencia a servicios anteriores)
```

### C.7.1 Comandos de Gestión Global

```
# Despliegue completo
cd /mnt/ssd/docker
docker-compose -f docker-compose-full.yml up -d

# Ver estado de todos los contenedores
```

```
docker ps -a

# Ver consumo de recursos
docker stats

# Logs agregados de todos los servicios
docker-compose -f docker-compose-full.yml logs -f

# Actualización OTA de todos los servicios
docker-compose -f docker-compose-full.yml pull
docker-compose -f docker-compose-full.yml up -d

# Detener todos los servicios
docker-compose -f docker-compose-full.yml down
```

## C.8 Resumen

Este anexo ha presentado los archivos Docker Compose completos para:

- OpenThread Border Router (OTBR)
- ThingsBoard Edge + PostgreSQL
- IEEE 2030.5 Server (SEP 2.0)
- Apache Kafka + Zookeeper
- Bridge Thread-ThingsBoard

Todos los servicios están configurados para:

- Reinicio automático (`restart: unless-stopped`)
- Logs rotados (max 10 MB, 3-5 archivos)
- Volúmenes persistentes en NVMe SSD
- Variables de entorno configurables via `.env`

Las implementaciones de código Python (IEEE 2030.5 Server, Bridge) se detallan en el Anexo C.

# D Anexo C: Scripts y Código de Integración

Este anexo presenta el código fuente completo de los componentes de software desarrollados para la integración de protocolos y servicios en el gateway. Incluye la implementación del servidor IEEE 2030.5, el bridge de traducción Thread-ThingsBoard, y los productores/consumidores Kafka.

## D.1 Servidor IEEE 2030.5 (SEP 2.0)

### D.1.1 Aplicación Flask Principal

Implementación del servidor RESTful IEEE 2030.5 en Python con Flask, proporcionando los Function Sets DCAP, Time y Metering Mirror.

app.py

```
from flask import Flask, Response, request
import requests
import json
import time
import os

app = Flask(__name__)

# Configuración ThingsBoard Edge
TB_EDGE_URL = os.getenv('TB_EDGE_URL', 'http://tb-edge:8080')
TB_EDGE_TOKEN = os.getenv('TB_EDGE_TOKEN', '')

# Namespace IEEE 2030.5
SEP_NS = 'urn:ieee:std:2030.5:ns'
```

```

@app.route('/dcap', methods=['GET'])
def device_capability():
    """
    IEEE 2030.5 Device Capability (DCAP)
    Endpoint de descubrimiento que expone los Function Sets disponibles.
    """
    xml = f'''<?xml version="1.0" encoding="UTF-8"?>
<DeviceCapability xmlns="{SEP_NS}">
    <href>/dcap</href>
    <TimeLink href="/tm"/>
    <MirrorUsagePointListLink href="/mup" all="0"/>
    <MessagingProgramListLink href="/msg" all="0"/>
    <EndDeviceListLink href="/edev" all="0"/>
    <SelfDeviceLink href="/sdev"/>
</DeviceCapability>'''
    return Response(xml, mimetype='application/sep+xml')

@app.route('/tm', methods=['GET'])
def time_sync():
    """
    IEEE 2030.5 Time (TM)
    Sincronización horaria para clientes SEP 2.0.
    Calidad 7 = máxima precisión (< 100ms vía NTP).
    """
    current_time = int(time.time())
    xml = f'''<?xml version="1.0" encoding="UTF-8"?>
<Time xmlns="{SEP_NS}">
    <currentTime>{current_time}</currentTime>
    <dstEndTime>0</dstEndTime>
    <dstOffset>0</dstOffset>
    <dstStartTime>0</dstStartTime>
    <localTime>{current_time}</localTime>
    <quality>7</quality>
    <tzOffset>-18000</tzOffset>
</Time>'''
    return Response(xml, mimetype='application/sep+xml')

@app.route('/mup', methods=['GET'])
def mirror_usage_point_list():
    """
    IEEE 2030.5 Mirror Usage Point List
    Lista de dispositivos con datos de medición disponibles.
    """
    # Consultar dispositivos en ThingsBoard Edge
    try:
        resp = requests.get(
            f"{TB_EDGE_URL}/api/tenant/devices?pageSize=100",
            headers={"X-Authorization": f"Bearer {TB_EDGE_TOKEN}"},
            timeout=5
        )
        devices = resp.json().get('data', [])
    except requests.exceptions.RequestException as e:
        print(f"Error al consultar dispositivos en ThingsBoard Edge: {e}")
        devices = []
    device_links = []
    for device in devices:
        device_links.append({
            "id": device['id'],
            "name": device['name'],
            "links": [
                {
                    "type": "mup",
                    "url": f"/mup/{device['id']}"
                }
            ]
        })
    return Response(json.dumps(device_links), mimetype='application/sep+xml')

```

```

        for idx, device in enumerate(devices):
            device_id = device['id']['id']
            device_links.append(
                f'    <MirrorUsagePoint href="/mup/{device_id}" />'
            )

        xml = f'''<?xml version="1.0" encoding="UTF-8"?>
<MirrorUsagePointList xmlns="{SEP_NS}" all="{len(devices)}">
{chr(10).join(device_links)}
</MirrorUsagePointList>'''
        return Response(xml, mimetype='application/sep+xml')

    except Exception as e:
        app.logger.error(f"Error fetching devices: {e}")
        return Response('Error fetching devices', status=500)

@app.route('/mup/<device_id>', methods=['GET'])
def mirror_usage_point(device_id):
    """
    IEEE 2030.5 Mirror Usage Point (individual device)
    Telemetría de medición reflejada desde ThingsBoard Edge.
    Granularidad: 15 minutos (900 segundos).
    """
    try:
        # Obtener últimas lecturas de telemetría
        resp = requests.get(
            f"{TB_EDGE_URL}/api/plugins/telemetry/DEVICE/{device_id}"
            "/values/timeseries?keys=energy_kwh,power_w,voltage_v",
            headers={"X-Authorization": f"Bearer {TB_EDGE_TOKEN}"},
            timeout=5
        )
        data = resp.json()

        # Extraer valores (último timestamp)
        energy_entry = data.get('energy_kwh', [{}])[0]
        power_entry = data.get('power_w', [{}])[0]
        voltage_entry = data.get('voltage_v', [{}])[0]

        energy_kwh = energy_entry.get('value', 0.0)
        power_w = power_entry.get('value', 0.0)
        voltage_v = voltage_entry.get('value', 0.0)
        timestamp = energy_entry.get('ts', int(time.time() * 1000)) // 1000

        # Convertir kWh a Wh (IEEE 2030.5 usa Wh entero)
        energy_wh = int(energy_kwh * 1000)

        xml = f'''<?xml version="1.0" encoding="UTF-8"?>
<MirrorUsagePoint xmlns="{SEP_NS}">
    <mRID>{device_id}</mRID>
    <deviceLFDI>{device_id[:16].upper()}</deviceLFDI>
    <MirrorMeterReading>
        <mRID>mr_{device_id}</mRID>
        <Reading>
            <value>{energy_wh}</value>

```

```

<localID>1</localID>
<timePeriod>
    <duration>900</duration>
    <start>{timestamp}</start>
</timePeriod>
</Reading>
<ReadingType>
    <powerOfTenMultiplier>0</powerOfTenMultiplier>
    < uom>72</ uom>
</ReadingType>
</MirrorMeterReading>
<MirrorMeterReading>
    <mRID>mr_p_{device_id}</mRID>
    <Reading>
        <value>{int(power_w)}</value>
        <localID>2</localID>
        <timePeriod>
            <duration>900</duration>
            <start>{timestamp}</start>
        </timePeriod>
    </Reading>
    <ReadingType>
        <powerOfTenMultiplier>0</powerOfTenMultiplier>
        < uom>38</ uom>
    </ReadingType>
</MirrorMeterReading>
</MirrorUsagePoint>'''
    return Response(xml, mimetype='application/sep+xml')

except Exception as e:
    app.logger.error(f"Error fetching telemetry for {device_id}: {e}")
    return Response('Device not found or telemetry unavailable',
                    status=404)

@app.route('/msg', methods=['GET'])
def messaging_program_list():
    """
    IEEE 2030.5 Messaging Program List
    Lista de programas de mensajería para alertas y notificaciones.
    """
    xml = f'''<?xml version="1.0" encoding="UTF-8"?>
<MessagingProgramList xmlns="{SEP_NS}" all="1">
    <MessagingProgram href="/msg/1">
        <mRID>msg-grid-alerts</mRID>
        <description>Grid Alerts and Notifications</description>
    </MessagingProgram>
</MessagingProgramList>'''
    return Response(xml, mimetype='application/sep+xml')

@app.route('/edev', methods=['GET'])
def end_device_list():
    """
    IEEE 2030.5 End Device List
    Lista de dispositivos registrados en el sistema.
    """

```

```

"""
try:
    resp = requests.get(
        f"{TB_EDGE_URL}/api/tenant/devices?pageSize=100",
        headers={"X-Authorization": f"Bearer {TB_EDGE_TOKEN}"},
        timeout=5
    )
    devices = resp.json().get('data', [])

    device_entries = []
    for device in devices:
        device_id = device['id']['id']
        device_name = device.get('name', 'Unknown')
        device_entries.append(f'''<EndDevice href="/edev/{device_id}">
<lFDI>{device_id[:16].upper()}</lFDI>
<sFDI>{device_id[:8]}</sFDI>
</EndDevice>'')

```

xml = f'''<?xml version="1.0" encoding="UTF-8"?>
<EndDeviceList xmlns="{SEP\_NS}" all="{len(devices)}">
{chr(10).join(device\_entries)}
</EndDeviceList>''
 return Response(xml, mimetype='application/sep+xml')

```

except Exception as e:
    app.logger.error(f"Error fetching devices: {e}")
    return Response('Error fetching devices', status=500)

if __name__ == '__main__':
    # Configuración TLS/mTLS
    cert_file = os.getenv('TLS_CERT', '/certs/server.crt')
    key_file = os.getenv('TLS_KEY', '/certs/server.key')

    app.run(
        host='0.0.0.0',
        port=8883,
        ssl_context=(cert_file, key_file),
        debug=False
    )

```

### D.1.2 Dockerfile

```

FROM python:3.11-slim

WORKDIR /app

# Dependencias del sistema
RUN apt-get update && apt-get install -y --no-install-recommends \
    ca-certificates \
&& rm -rf /var/lib/apt/lists/*

```

```

# Dependencias Python
COPY requirements.txt .
RUN pip install --no-cache-dir -r requirements.txt

# Código de aplicación
COPY app.py .

# Usuario no privilegiado
RUN useradd -m -u 1000 sepuser && \
    chown -R sepuser:sepuser /app
USER sepuser

EXPOSE 8883

CMD ["python", "app.py"]

```

### D.1.3 requirements.txt

```

Flask==3.0.0
requests==2.31.0
pyOpenSSL==23.3.0
Werkzeug==3.0.1

```

## D.2 Bridge Thread ↔ ThingsBoard Edge

### D.2.1 Script Bridge Principal

Traductor de protocolos que convierte mensajes CoAP/MQTT desde dispositivos Thread a formato ThingsBoard.

#### bridge.py

```

import paho.mqtt.client as mqtt
import json
import time
import logging
import os

# Configuración de logging
logging.basicConfig(

```

```

    level=logging.INFO,
    format='%(asctime)s - %(name)s - %(levelname)s - %(message)s'
)
logger = logging.getLogger(__name__)

# Configuración MQTT
THREAD_BROKER = os.getenv('THREAD_BROKER', 'localhost')
THREAD_PORT = int(os.getenv('THREAD_PORT', '1883'))
THREAD_TOPIC = os.getenv('THREAD_TOPIC', 'thread/telemetry/#')

TB_BROKER = os.getenv('TB_BROKER', 'localhost')
TB_PORT = int(os.getenv('TB_PORT', '1883'))
TB_ACCESS_TOKEN = os.getenv('TB_ACCESS_TOKEN', '')

# Cliente MQTT para dispositivos Thread
thread_client = mqtt.Client(client_id='thread_bridge')

# Cliente MQTT para ThingsBoard Edge
tb_client = mqtt.Client(client_id='tb_bridge')

# Contador de mensajes procesados
message_count = 0
last_log_time = time.time()

def on_thread_connect(client, userdata, flags, rc):
    """Callback al conectar con broker Thread"""
    if rc == 0:
        logger.info(f"Connected to Thread MQTT broker at {THREAD_BROKER}")
        client.subscribe(THREAD_TOPIC)
        logger.info(f"Subscribed to {THREAD_TOPIC}")
    else:
        logger.error(f"Failed to connect to Thread broker, code {rc}")

def on_tb_connect(client, userdata, flags, rc):
    """Callback al conectar con ThingsBoard Edge"""
    if rc == 0:
        logger.info(f"Connected to ThingsBoard Edge at {TB_BROKER}")
    else:
        logger.error(f"Failed to connect to TB Edge, code {rc}")

def transform_telemetry(thread_data):
    """
    Transforma datos de Thread a formato ThingsBoard.

    Thread input format:
    {
        "device_id": "esp32c6_001",
        "timestamp": 1730000000,
        "temperature_c": 25.3,
        "humidity_pct": 65.8,
        "energy_kwh": 12.456,
        "power_w": 1250,
        "voltage_v": 230.5
    }
    """

```

```

ThingsBoard output format:
{
    "ts": 1730000000000, # Milliseconds
    "values": {
        "temperature": 25.3,
        "humidity": 65.8,
        "energy": 12.456,
        "power": 1250,
        "voltage": 230.5
    }
}
"""
try:
    # Convertir timestamp a milisegundos
    ts_ms = int(thread_data.get('timestamp', time.time()) * 1000

    # Mapear campos a formato TB
    telemetry = {
        "ts": ts_ms,
        "values": {}
    }

    # Mapeo de campos comunes
    field_mapping = {
        'temperature_c': 'temperature',
        'humidity_pct': 'humidity',
        'energy_kwh': 'energy',
        'power_w': 'power',
        'voltage_v': 'voltage',
        'current_a': 'current',
        'frequency_hz': 'frequency',
        'pf': 'powerFactor'
    }

    for thread_key, tb_key in field_mapping.items():
        if thread_key in thread_data:
            telemetry['values'][tb_key] = thread_data[thread_key]

    return telemetry

except Exception as e:
    logger.error(f"Error transforming telemetry: {e}")
    return None

def on_thread_message(client, userdata, msg):
    """
    Callback al recibir mensaje de dispositivos Thread.
    Transforma y publica a ThingsBoard Edge.
    """
    global message_count, last_log_time

    try:
        # Decodificar payload

```

```

payload_str = msg.payload.decode('utf-8')
thread_data = json.loads(payload_str)

logger.debug(f"Received from Thread: {thread_data}")

# Extraer device_id del mensaje o del topic
device_id = thread_data.get('device_id')
if not device_id:
    # Extraer de topic: thread/telemetry/device123 -> device123
    topic_parts = msg.topic.split('/')
    if len(topic_parts) >= 3:
        device_id = topic_parts[2]
    else:
        logger.warning("No device_id found in message or topic")
        return

# Transformar datos
tb_telemetry = transform_telemetry(thread_data)
if not tb_telemetry:
    return

# Publicar a ThingsBoard Edge
tb_topic = f"v1/devices/{device_id}/telemetry"
tb_payload = json.dumps(tb_telemetry)

result = tb_client.publish(tb_topic, tb_payload, qos=1)

if result.rc == mqtt.MQTT_ERR_SUCCESS:
    message_count += 1

    # Log estadísticas cada 100 mensajes
    if message_count % 100 == 0:
        elapsed = time.time() - last_log_time
        rate = 100 / elapsed if elapsed > 0 else 0
        logger.info(f"Processed {message_count} messages "
                   f"({rate:.1f} msg/s)")
        last_log_time = time.time()
else:
    logger.error(f"Failed to publish to TB: {result.rc}")

except json.JSONDecodeError as e:
    logger.error(f"Invalid JSON from Thread: {e}")
except Exception as e:
    logger.error(f"Error processing Thread message: {e}")

def main():
    """Función principal del bridge"""
    logger.info("Starting Thread-ThingsBoard Bridge...")

    # Configurar callbacks Thread
    thread_client.on_connect = on_thread_connect
    thread_client.on_message = on_thread_message

    # Configurar callbacks ThingsBoard

```

```

tb_client.on_connect = on_tb_connect
tb_client.username_pw_set(TB_ACCESS_TOKEN)

# Conectar a ambos brokers
try:
    logger.info(f"Connecting to Thread broker {THREAD_BROKER}:{THREAD_PORT}")
    thread_client.connect(THREAD_BROKER, THREAD_PORT, keepalive=60)

    logger.info(f"Connecting to TB Edge {TB_BROKER}:{TB_PORT}")
    tb_client.connect(TB_BROKER, TB_PORT, keepalive=60)

    # Iniciar loops en threads separados
    thread_client.loop_start()
    tb_client.loop_start()

    logger.info("Bridge is running. Press Ctrl+C to stop.")

    # Mantener vivo
    while True:
        time.sleep(1)

except KeyboardInterrupt:
    logger.info("Shutting down bridge...")
except Exception as e:
    logger.error(f"Fatal error: {e}")
finally:
    thread_client.loop_stop()
    tb_client.loop_stop()
    thread_client.disconnect()
    tb_client.disconnect()
    logger.info("Bridge stopped.")

if __name__ == '__main__':
    main()

```

## D.2.2 Dockerfile del Bridge

```

FROM python:3.11-slim

WORKDIR /app

# Dependencias Python
COPY requirements_bridge.txt requirements.txt
RUN pip install --no-cache-dir -r requirements.txt

# Script bridge
COPY bridge.py .

# Usuario no privilegiado
RUN useradd -m -u 1000 bridgeuser && \

```

```
chown -R bridgeuser:bridgeuser /app
USER bridgeuser

CMD ["python", "bridge.py"]
```

### D.2.3 requirements\_bridge.txt

```
paho-mqtt==1.6.1
```

## D.3 Integración con Apache Kafka

### D.3.1 Productor Kafka

Versión mejorada del bridge que publica telemetría a Kafka para procesamiento distribuido.

#### kafka\_producer.py

```
from kafka import KafkaProducer
import paho.mqtt.client as mqtt
import json
import time
import logging
import os

logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)

# Configuración Kafka
KAFKA_BOOTSTRAP = os.getenv('KAFKA_BOOTSTRAP', 'localhost:9092')
KAFKA_TOPIC = os.getenv('KAFKA_TOPIC', 'telemetry')
KAFKA_COMPRESSION = os.getenv('KAFKA_COMPRESSION', 'lz4')

# Configuración MQTT Thread
THREAD_BROKER = os.getenv('THREAD_BROKER', 'localhost')
THREAD_PORT = int(os.getenv('THREAD_PORT', '1883'))
THREAD_TOPIC = os.getenv('THREAD_TOPIC', 'thread/telemetry/#')

# Inicializar productor Kafka
producer = KafkaProducer(
    bootstrap_servers=KAFKA_BOOTSTRAP.split(','),
    value_serializer=lambda v: json.dumps(v).encode('utf-8'),
```

```

compression_type=KAFKA_COMPRESSION,
acks='all', # Confirmación de todas las réplicas
retries=3,
max_in_flight_requests_per_connection=5,
linger_ms=100, # Batching: esperar 100ms para agrupar mensajes
batch_size=16384 # 16 KB batch size
)

# Cliente MQTT
mqtt_client = mqtt.Client(client_id='kafka_producer')

def on_connect(client, userdata, flags, rc):
    if rc == 0:
        logger.info(f"Connected to Thread MQTT at {THREAD_BROKER}")
        client.subscribe(THREAD_TOPIC)
    else:
        logger.error(f"MQTT connection failed: {rc}")

def on_message(client, userdata, msg):
    """Recibir de Thread, publicar a Kafka"""
    try:
        payload = json.loads(msg.payload.decode('utf-8'))

        # Enriquecer con metadata
        kafka_message = {
            'device_id': payload.get('device_id', 'unknown'),
            'timestamp': int(time.time() * 1000), # ms
            'source_topic': msg.topic,
            'data': payload
        }

        # Publicar a Kafka
        future = producer.send(KAFKA_TOPIC, kafka_message)

        # Callback opcional para confirmar
        future.add_callback(lambda metadata:
            logger.debug(f"Sent to {metadata.topic}:{metadata.partition} "
                         f"offset {metadata.offset}"))
        future.add_errback(lambda e:
            logger.error(f"Kafka send failed: {e}"))

    except Exception as e:
        logger.error(f"Error processing message: {e}")

def main():
    logger.info(f"Kafka Producer starting...")
    logger.info(f"Kafka: {KAFKA_BOOTSTRAP} | Topic: {KAFKA_TOPIC}")
    logger.info(f"MQTT: {THREAD_BROKER}:{THREAD_PORT} | Topic: {THREAD_TOPIC}")

    mqtt_client.on_connect = on_connect
    mqtt_client.on_message = on_message

    try:
        mqtt_client.connect(THREAD_BROKER, THREAD_PORT, keepalive=60)

```

```

    mqtt_client.loop_start()

    logger.info("Producer running. Press Ctrl+C to stop.")
    while True:
        time.sleep(1)

    except KeyboardInterrupt:
        logger.info("Shutting down...")
    finally:
        producer.flush()
        producer.close()
        mqtt_client.loop_stop()
        mqtt_client.disconnect()

if __name__ == '__main__':
    main()

```

### D.3.2 Consumidor Kafka

Consumidor que lee de Kafka y publica a ThingsBoard Edge.

#### kafka\_consumer.py

```

from kafka import KafkaConsumer
import paho.mqtt.client as mqtt
import json
import logging
import os

logging.basicConfig(level=logging.INFO)
logger = logging.getLogger(__name__)

# Configuración Kafka
KAFKA_BOOTSTRAP = os.getenv('KAFKA_BOOTSTRAP', 'localhost:9092')
KAFKA_TOPIC = os.getenv('KAFKA_TOPIC', 'telemetry')
KAFKA_GROUP_ID = os.getenv('KAFKA_GROUP_ID', 'tb-edge-consumer')

# Configuración ThingsBoard
TB_BROKER = os.getenv('TB_BROKER', 'localhost')
TB_PORT = int(os.getenv('TB_PORT', '1883'))
TB_ACCESS_TOKEN = os.getenv('TB_ACCESS_TOKEN', '')

# Consumer Kafka
consumer = KafkaConsumer(
    KAFKA_TOPIC,
    bootstrap_servers=KAFKA_BOOTSTRAP.split(','),
    group_id=KAFKA_GROUP_ID,

```

```

        value_deserializer=lambda m: json.loads(m.decode('utf-8')),
        auto_offset_reset='earliest', # Procesar desde el inicio si es nuevo
        enable_auto_commit=True,
        auto_commit_interval_ms=5000
    )

# Cliente MQTT ThingsBoard
tb_client = mqtt.Client(client_id='kafka_consumer')
tb_client.username_pw_set(TB_ACCESS_TOKEN)

def on_tb_connect(client, userdata, flags, rc):
    if rc == 0:
        logger.info(f"Connected to ThingsBoard Edge at {TB_BROKER}")
    else:
        logger.error(f"TB connection failed: {rc}")

def main():
    logger.info(f"Kafka Consumer starting...")
    logger.info(f"Kafka: {KAFKA_BOOTSTRAP} | Topic: {KAFKA_TOPIC} | "
               f"Group: {KAFKA_GROUP_ID}")
    logger.info(f"ThingsBoard: {TB_BROKER}:{TB_PORT}")

    tb_client.on_connect = on_tb_connect
    tb_client.connect(TB_BROKER, TB_PORT, keepalive=60)
    tb_client.loop_start()

    try:
        logger.info("Consuming messages from Kafka...")
        for message in consumer:
            try:
                kafka_data = message.value
                device_id = kafka_data.get('device_id', 'unknown')
                payload = kafka_data.get('data', {})

                # Transformar a formato TB
                tb_telemetry = {
                    'ts': kafka_data.get('timestamp'),
                    'values': payload
                }

                # Publicar a TB Edge
                tb_topic = f"v1/devices/{device_id}/telemetry"
                tb_client.publish(tb_topic, json.dumps(tb_telemetry), qos=1)

                logger.debug(f"Forwarded device {device_id} to TB Edge")

            except Exception as e:
                logger.error(f"Error processing Kafka message: {e}")

    except KeyboardInterrupt:
        logger.info("Shutting down...")
    finally:
        consumer.close()
        tb_client.loop_stop()

```

```

tb_client.disconnect()

if __name__ == '__main__':
    main()

```

### D.3.3 requirements\_kafka.txt

```

kafka-python==2.0.2
paho-mqtt==1.6.1

```

## D.4 Scripts de Gestión

### D.4.1 Comandos de Verificación

#### verify\_services.sh

```

#!/bin/bash
# Script para verificar estado de servicios del gateway

echo "==== Gateway Services Status ==="

# Docker containers
echo -e "\n[Docker Containers]"
docker ps --format "table {{.Names}}\t{{.Status}}\t{{.Ports}}"

# OpenThread Border Router
echo -e "\n[OpenThread RCP]"
docker exec -it otbr ot-ctl state 2>/dev/null || echo "OTBR not running"

# ThingsBoard Edge
echo -e "\n[ThingsBoard Edge]"
curl -s http://localhost:8080/api/auth/token -o /dev/null && \
echo "TB Edge: Running" || echo "TB Edge: Not accessible"

# IEEE 2030.5 Server
echo -e "\n[IEEE 2030.5 Server]"
curl -k -s https://localhost:8883/dcap -o /dev/null && \
echo "SEP 2.0 Server: Running" || echo "SEP 2.0 Server: Not accessible"

# Kafka
echo -e "\n[Kafka Topics]"
docker exec -it kafka kafka-topics --list \
--bootstrap-server localhost:9092 2>/dev/null || \

```

```

echo "Kafka not running"

# Network interfaces
echo -e "\n[Network Interfaces]"
ip -br addr show | grep -E 'wlan|wpan|wwan|eth'

echo -e "\n==== End of Status Check ==="

```

#### D.4.2 Backup de Configuraciones

`backup_config.sh`

```

#!/bin/bash
# Backup de configuraciones del gateway

BACKUP_DIR="/mnt/ssd/backups"
TIMESTAMP=$(date +%Y%m%d_%H%M%S)
BACKUP_FILE="$BACKUP_DIR/gateway_backup_${TIMESTAMP}.tar.gz"

mkdir -p "$BACKUP_DIR"

echo "Creating gateway configuration backup..."

tar -czf "$BACKUP_FILE" \
    /etc/config \
    /mnt/ssd/docker/*/*docker-compose.yml \
    /mnt/ssd/docker/*/*.py \
    /mnt/ssd/docker/*/*certs \
    2>/dev/null

if [ $? -eq 0 ]; then
    echo "Backup created: $BACKUP_FILE"
    ls -lh "$BACKUP_FILE"

    # Mantener solo últimos 7 backups
    ls -t "$BACKUP_DIR"/gateway_backup_*.tar.gz | tail -n +8 | xargs rm -f
else
    echo "Backup failed"
    exit 1
fi

```

# E Anexo D: Especificaciones IEEE 2030.5 y Configuraciones

Este anexo documenta las especificaciones completas de configuración para los componentes del gateway, incluyendo ejemplos XML IEEE 2030.5, comandos UCI para HaLow, y optimizaciones para TimescaleDB.

## E.1 Ejemplos XML IEEE 2030.5

### E.1.1 Device Capability (DCAP)

Documento XML completo del endpoint de descubrimiento de capacidades:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceCapability xmlns="urn:ieee:std:2030.5:ns">
    <href>/dcap</href>
    <pollRate>900</pollRate>
    <TimeLink href="/tm"/>
    <MirrorUsagePointListLink href="/mup" all="0"/>
    <MessagingProgramListLink href="/msg" all="0"/>
    <EndDeviceListLink href="/edev" all="0"/>
    <DERProgramListLink href="/derp" all="0"/>
    <SelfDeviceLink href="/sdev"/>
</DeviceCapability>
```

### E.1.2 Time Synchronization (TM)

Respuesta de sincronización horaria con calidad máxima:

```
<?xml version="1.0" encoding="UTF-8"?>
<Time xmlns="urn:ieee:std:2030.5:ns">
  <currentTime>1730000000</currentTime>
  <dstEndTime>1698627600</dstEndTime>
  <dstOffset>3600</dstOffset>
  <dstStartTime>1710046800</dstStartTime>
  <localTime>1730000000</localTime>
  <quality>7</quality>
  <tzOffset>-18000</tzOffset>
</Time>
```

#### Campos importantes:

- **currentTime**: Tiempo UNIX en segundos (UTC).
- **quality**: 0-7, donde 7 indica sincronización NTP con precisión <100 ms.
- **tzOffset**: Offset en segundos desde UTC (Colombia: -18000 = UTC-5).
- **dstOffset**: Offset adicional durante horario de verano (si aplica).

### E.1.3 Mirror Usage Point (MUP)

Ejemplo de telemetría de medición reflejada:

```
<?xml version="1.0" encoding="UTF-8"?>
<MirrorUsagePoint xmlns="urn:ieee:std:2030.5:ns">
  <mRID>0123456789ABCDEF0123456789ABCDEF</mRID>
  <deviceLFDI>0123456789ABCDEF</deviceLFDI>
  <MirrorMeterReading>
    <mRID>mr_energy_001</mRID>
    <description>Active Energy Delivered</description>
    <Reading>
      <consumptionBlock>0</consumptionBlock>
      <qualityFlags>0</qualityFlags>
      <timePeriod>
        <duration>900</duration>
        <start>1730000000</start>
      </timePeriod>
      <touTier>0</touTier>
      <value>123456789</value>
      <localID>1</localID>
    </Reading>
    <ReadingType>
      <accumulationBehaviour>4</accumulationBehaviour>
      <commodity>1</commodity>
      <dataQualifier>0</dataQualifier>
```

```

<flowDirection>1</flowDirection>
<intervalLength>900</intervalLength>
<kind>12</kind>
<phase>0</phase>
<powerOfTenMultiplier>0</powerOfTenMultiplier>
<timeAttribute>0</timeAttribute>
<uom>72</uom>
</ReadingType>
</MirrorMeterReading>
<MirrorMeterReading>
<mRID>mr_power_001</mRID>
<description>Instantaneous Active Power</description>
<Reading>
<qualityFlags>0</qualityFlags>
<timePeriod>
<duration>900</duration>
<start>1730000000</start>
</timePeriod>
<value>1250</value>
<localID>2</localID>
</Reading>
<ReadingType>
<accumulationBehaviour>0</accumulationBehaviour>
<commodity>1</commodity>
<dataQualifier>0</dataQualifier>
<flowDirection>1</flowDirection>
<intervalLength>0</intervalLength>
<kind>12</kind>
<phase>0</phase>
<powerOfTenMultiplier>0</powerOfTenMultiplier>
<timeAttribute>0</timeAttribute>
<uom>38</uom>
</ReadingType>
</MirrorMeterReading>
<MirrorMeterReading>
<mRID>mr_voltage_001</mRID>
<description>RMS Voltage</description>
<Reading>
<qualityFlags>0</qualityFlags>
<timePeriod>
<duration>900</duration>
<start>1730000000</start>
</timePeriod>
<value>2305</value>
<localID>3</localID>
</Reading>
<ReadingType>
<accumulationBehaviour>0</accumulationBehaviour>
<commodity>1</commodity>
<dataQualifier>0</dataQualifier>
<flowDirection>1</flowDirection>
<intervalLength>0</intervalLength>
<kind>12</kind>
<phase>0</phase>

```

```

<powerOfTenMultiplier>-1</powerOfTenMultiplier>
<timeAttribute>0</timeAttribute>
<uom>29</uom>
</ReadingType>
</MirrorMeterReading>
</MirrorUsagePoint>

```

#### **ReadingType - Unidades de Medida (uom):**

- 38: Watts (W) - Potencia activa
- 72: Watt-hours (Wh) - Energía activa
- 29: Voltage (V) - Voltaje RMS
- 5: Current (A) - Corriente RMS
- 63: Volt-Ampere Reactive (VAr) - Potencia reactiva

#### **E.1.4 End Device List**

Lista de dispositivos registrados con identificadores LFDI/SFDI:

```

<?xml version="1.0" encoding="UTF-8"?>
<EndDeviceList xmlns="urn:ieee:std:2030.5:ns" all="3">
  <EndDevice href="/edev/001">
    <changedTime>1730000000</changedTime>
    <enabled>true</enabled>
    <lFDI>0123456789ABCDEF</lFDI>
    <sFDI>01234567</sFDI>
    <FunctionSetAssignmentsListLink href="/edev/001/fsa" all="4"/>
    <RegistrationLink href="/edev/001/rg"/>
  </EndDevice>
  <EndDevice href="/edev/002">
    <changedTime>1730001000</changedTime>
    <enabled>true</enabled>
    <lFDI>FEDCBA9876543210</lFDI>
    <sFDI>FEDCBA98</sFDI>
    <FunctionSetAssignmentsListLink href="/edev/002/fsa" all="4"/>
    <RegistrationLink href="/edev/002/rg"/>
  </EndDevice>
  <EndDevice href="/edev/003">
    <changedTime>1730002000</changedTime>
    <enabled>true</enabled>
    <lFDI>1234567890ABCDEF</lFDI>
    <sFDI>12345678</sFDI>
    <FunctionSetAssignmentsListLink href="/edev/003/fsa" all="4"/>
    <RegistrationLink href="/edev/003/rg"/>
  </EndDevice>
</EndDeviceList>

```

```
</EndDevice>  
</EndDeviceList>
```

## E.2 Configuraciones UCI para HaLow 802.11ah

### E.2.1 Modo Access Point (AP)

Configuración completa del gateway como AP HaLow:

```
# Interfaz inalámbrica HaLow (wlan2)  
uci set wireless.hallow=wifi-device  
uci set wireless.hallow.type='mac80211'  
uci set wireless.hallow.path='platform/soc/1e140000.pcie/pci0000:00/0000:00:00.0/0000:01:00.0'  
uci set wireless.hallow.channel='7'          # 917 MHz (S1G)  
uci set wireless.hallow.bandwidth='8'        # 8 MHz (opciones: 1, 2, 4, 8, 16)  
uci set wireless.hallow.hwmode='11ah'  
uci set wireless.hallow.country='US'  
uci set wireless.hallow.txpower='20'         # 20 dBm = 100 mW  
uci set wireless.hallow.legacy_rates='0'  
uci set wireless.hallow.mu_beamformer='0'  
uci set wireless.hallow.mu_beamformee='0'  
  
# Interfaz virtual AP  
uci set wireless.hallow_ap=wifi-iface  
uci set wireless.hallow_ap.device='hallow'  
uci set wireless.hallow_ap.mode='ap'  
uci set wireless.hallow_ap.network='hallow_lan'  
uci set wireless.hallow_ap.ssid='SmartGrid-HaLow-AP'  
uci set wireless.hallow_ap.encryption='sae'  
uci set wireless.hallow_ap.key='<WPA3-PSK-SECURE-KEY>'  
uci set wireless.hallow_ap.ieee80211w='2'  # PMF obligatorio  
uci set wireless.hallow_ap.sae_pwe='2'      # Hash-to-Element (H2E)  
uci set wireless.hallow_ap.wpa_disable_eapol_key_retries='1'  
uci set wireless.hallow_ap.max_inactivity='600' # 10 min timeout  
uci set wireless.hallow_ap.disassoc_low_ack='0'  
uci set wireless.hallow_ap.skip_inactivity_poll='0'  
  
# Red virtual para HaLow  
uci set network.hallow_lan=interface  
uci set network.hallow_lan.proto='static'  
uci set network.hallow_lan.ipaddr='192.168.100.1'  
uci set network.hallow_lan.netmask='255.255.255.0'  
uci set network.hallow_lan.ip6assign='64'  
uci set network.hallow_lan.ip6hint='100'  
  
# DHCP server para clientes HaLow
```

```

uci set dhcp.hallow=dhcp
uci set dhcp.hallow.interface='halow_lan'
uci set dhcp.hallow.start='100'
uci set dhcp.hallow.limit='150'
uci set dhcp.hallow.leasetime='12h'
uci set dhcp.hallow.dhcpv6='server'
uci set dhcp.hallow.ra='server'
uci set dhcp.hallow.ra_management='1'

# Firewall zone
uci set firewall.hallow_zone=zone
uci set firewall.hallow_zone.name='halow'
uci set firewall.hallow_zone.input='ACCEPT'
uci set firewall.hallow_zone.output='ACCEPT'
uci set firewall.hallow_zone.forward='ACCEPT'
uci set firewall.hallow_zone.network='halow_lan'

uci set firewall.hallow_lan_forwarding=forwarding
uci set firewall.hallow_lan_forwarding.src='halow'
uci set firewall.hallow_lan_forwarding.dest='lan'

uci set firewall.hallow_wan_forwarding=forwarding
uci set firewall.hallow_wan_forwarding.src='halow'
uci set firewall.hallow_wan_forwarding.dest='wan'

# Aplicar configuración
uci commit wireless
uci commit network
uci commit dhcp
uci commit firewall

# Reiniciar servicios
wifi reload
/etc/init.d/network restart
/etc/init.d/firewall restart

```

## E.2.2 Modo Station (STA)

Configuración del gateway para conectarse a AP HaLow remoto:

```

# Interfaz HaLow como Station
uci set wireless.hallow=wifi-device
uci set wireless.hallow.type='mac80211'
uci set wireless.hallow.channel='auto'      # Auto-scan
uci set wireless.hallow.bandwidth='8'
uci set wireless.hallow.hwmode='11ah'
uci set wireless.hallow.country='US'
uci set wireless.hallow.disabled='0'

```

## E.2. Configuraciones UCI para HaLow 802.1Eah Anexo D: Especificaciones IEEE 2030.5 y Configuraciones

```
uci set wireless.halow_sta=wifi-iface
uci set wireless.halow_sta.device='halow'
uci set wireless.halow_sta.mode='sta'
uci set wireless.halow_sta.network='wan_halow'
uci set wireless.halow_sta.ssid='SmartGrid-HaLow-Backhaul'
uci set wireless.halow_sta.encryption='sae'
uci set wireless.halow_sta.key='<WPA3-PSK-BACKHAUL>'
uci set wireless.halow_sta.ieee80211w='2'

# Red WAN via HaLow
uci set network.wan_halow=interface
uci set network.wan_halow.proto='dhcp'
uci set network.wan_halow.metric='20' # Métrica menor = mayor prioridad

# Agregar a mwan3 para failover
uci set mwan3.wan_halow=interface
uci set mwan3.wan_halow.enabled='1'
uci set mwan3.wan_halow.family='ipv4'
uci set mwan3.wan_halow.track_ip='8.8.8.8'
uci set mwan3.wan_halow.track_ip='1.1.1.1'
uci set mwan3.wan_halow.track_method='ping'
uci set mwan3.wan_halow.reliability='1'
uci set mwan3.wan_halow.count='1'
uci set mwan3.wan_halow.size='56'
uci set mwan3.wan_halow.max_ttl='60'
uci set mwan3.wan_halow.timeout='2'
uci set mwan3.wan_halow.interval='5'
uci set mwan3.wan_halow.down='3'
uci set mwan3.wan_halow.up='3'

uci commit wireless
uci commit network
uci commit mwan3

wifi reload
/etc/init.d/network restart
/etc/init.d/mwan3 restart
```

### E.2.3 Modo Mesh 802.11s

Configuración para red mesh sin controlador centralizado:

```
# Interfaz HaLow Mesh
uci set wireless.halow=wifi-device
uci set wireless.halow.type='mac80211'
uci set wireless.halow.channel='7'
uci set wireless.halow.bandwidth='8'
uci set wireless.halow.hwmode='11ah'
uci set wireless.halow.country='US'
```

```

uci set wireless.halow.txpower='20'

uci set wireless.halow_mesh=wifi-iface
uci set wireless.halow_mesh.device='halow'
uci set wireless.halow_mesh.mode='mesh'
uci set wireless.halow_mesh.mesh_id='smartgrid-mesh'
uci set wireless.halow_mesh.mesh_fwding='1'
uci set wireless.halow_mesh.mesh_ttl='31'
uci set wireless.halow_mesh.mesh_rssi_threshold='-80'
uci set wireless.halow_mesh.encryption='sae'
uci set wireless.halow_mesh.key='<MESH-KEY>'
uci set wireless.halow_mesh.network='mesh_lan'

# Red mesh
uci set network.mesh_lan=interface
uci set network.mesh_lan.proto='batadv_hardif'
uci set network.mesh_lan.master='bat0'
uci set network.mesh_lan.mtu='1532'

uci set network.bat0=interface
uci set network.bat0.proto='static'
uci set network.bat0.ipaddr='10.100.0.1'
uci set network.bat0.netmask='255.255.0.0'
uci set network.bat0.ip6assign='64'

# Batman-adv
uci set batman-adv.bat0=mesh
uci set batman-adv.bat0.aggregated_ogms='1'
uci set batman-adv.bat0.ap_isolation='0'
uci set batman-adv.bat0.bonding='0'
uci set batman-adv.bat0.fragmentation='1'
uci set batman-adv.bat0.gw_mode='server'
uci set batman-adv.bat0.log_level='0'
uci set batman-adv.bat0.orig_interval='5000'
uci set batman-adv.bat0.bridge_loop_avoidance='1'
uci set batman-adv.bat0.distributed_arp_table='1'
uci set batman-adv.bat0.multicast_mode='1'

uci commit wireless
uci commit network
uci commit batman-adv

# Cargar módulo kernel
modprobe batman-adv

wifi reload
/etc/init.d/network restart

```

## E.2.4 Modo EasyMesh (IEEE 1905.1)

Configuración para mesh gestionado con controlador y agentes:

```

# Controlador EasyMesh (Gateway principal)
uci set easymesh.config=easymesh
uci set easymesh.config.enabled='1'
uci set easymesh.config.role='controller'

# Interfaz backhaul HaLow
uci set wireless.halow_backhaul=wifi-iface
uci set wireless.halow_backhaul.device='halow'
uci set wireless.halow_backhaul.mode='ap'
uci set wireless.halow_backhaul.network='backhaul'
uci set wireless.halow_backhaul.ssid='mesh-backhaul-5g'
uci set wireless.halow_backhaul.encryption='sae'
uci set wireless.halow_backhaul.key='<BACKHAUL-KEY>'
uci set wireless.halow_backhaul.multi_ap='2' # Backhaul BSS
uci set wireless.halow_backhaul.ieee80211w='2'
uci set wireless.halow_backhaul.hidden='1'

# Interfaz frontal para clientes
uci set wireless.halow_front=wifi-iface
uci set wireless.halow_front.device='halow'
uci set wireless.halow_front.mode='ap'
uci set wireless.halow_front.network='lan'
uci set wireless.halow_front.ssid='SmartGrid-HaLow'
uci set wireless.halow_front.encryption='sae'
uci set wireless.halow_front.key='<CLIENT-KEY>'
uci set wireless.halow_front.multi_ap='1' # Fronthaul BSS
uci set wireless.halow_front.ieee80211w='2'

# Red backhaul
uci set network.backhaul=interface
uci set network.backhaul.proto='static'
uci set network.backhaul.ipaddr='192.168.200.1'
uci set network.backhaul.netmask='255.255.255.0'

# Servicios EasyMesh
uci set ieee1905.ieee1905=ieee1905
uci set ieee1905.ieee1905.enabled='1'
uci set ieee1905.ieee1905.al_interface='eth0'
uci set ieee1905.ieee1905.management_interface='br-lan'

uci commit easymesh
uci commit wireless
uci commit network
uci commit ieee1905

/etc/init.d/easymesh enable
/etc/init.d/easymesh start

```

```
wifi reload
```

## E.3 Optimización TimescaleDB

### E.3.1 Configuración PostgreSQL + TimescaleDB

Optimizaciones para almacenamiento de series temporales de alta frecuencia:

```
# postgresql.conf (dentro del contenedor)
# Ubicación: /var/lib/postgresql/data/postgresql.conf

# --- Memoria ---
shared_buffers = 2GB          # 25% de RAM (para RPi4 8GB)
effective_cache_size = 6GB    # 75% de RAM
work_mem = 16MB               # Por operación de sort/hash
maintenance_work_mem = 512MB  # Para VACUUM, CREATE INDEX

# --- Escritura ---
wal_buffers = 16MB
checkpoint_completion_target = 0.9
max_wal_size = 4GB
min_wal_size = 1GB
wal_compression = on

# --- Checkpoints (reducir I/O en SSD) ---
checkpoint_timeout = 30min
checkpoint_warning = 5min

# --- Queries ---
random_page_cost = 1.1        # SSD, no HDD
effective_io_concurrency = 200 # Para NVMe
max_worker_processes = 4      # CPUs disponibles
max_parallel_workers_per_gather = 2
max_parallel_workers = 4

# --- Logging ---
logging_collector = on
log_destination = 'csvlog'
log_directory = 'log'
log_filename = 'postgresql-%Y-%m-%d.log'
log_rotation_age = 1d
log_rotation_size = 100MB
log_min_duration_statement = 1000 # Log queries > 1s

# --- TimescaleDB ---
shared_preload_libraries = 'timescaledb'
timescaledb.max_background_workers = 4
```

### E.3.2 Schema y Hypertables

Creación de tablas optimizadas para telemetría:

```
-- Crear extensión TimescaleDB
CREATE EXTENSION IF NOT EXISTS timescaledb;

-- Tabla principal de telemetría
CREATE TABLE telemetry (
    time      TIMESTAMPTZ NOT NULL,
    device_id TEXT NOT NULL,
    metric    TEXT NOT NULL,
    value     DOUBLE PRECISION,
    unit      TEXT,
    quality   SMALLINT DEFAULT 0
);

-- Convertir a hypertable (particionado automático por tiempo)
SELECT create_hypertable('telemetry', 'time',
    chunk_time_interval => INTERVAL '1 day');

-- Índices para queries frecuentes
CREATE INDEX idx_telemetry_device_time ON telemetry (device_id, time DESC);
CREATE INDEX idx_telemetry_metric_time ON telemetry (metric, time DESC);

-- Compresión automática (chunks > 7 días)
ALTER TABLE telemetry SET (
    timescaledb.compress,
    timescaledb.compress_segmentby = 'device_id,metric',
    timescaledb.compress_orderby = 'time DESC'
);

SELECT add_compression_policy('telemetry', INTERVAL '7 days');

-- Retención automática (eliminar datos > 1 año)
SELECT add_retention_policy('telemetry', INTERVAL '365 days');

-- Continuous Aggregates (vistas materializadas)
CREATE MATERIALIZED VIEW telemetry_15min
WITH (timescaledb.continuous) AS
SELECT time_bucket('15 minutes', time) AS bucket,
       device_id,
       metric,
       AVG(value) AS avg_value,
       MAX(value) AS max_value,
       MIN(value) AS min_value,
       COUNT(*) AS sample_count
FROM telemetry
GROUP BY bucket, device_id, metric
WITH NO DATA;
```

```
-- Refrescar cada 5 minutos
SELECT add_continuous_aggregate_policy('telemetry_15min',
    start_offset => INTERVAL '1 hour',
    end_offset => INTERVAL '5 minutes',
    schedule_interval => INTERVAL '5 minutes');

-- Vista agregada horaria
CREATE MATERIALIZED VIEW telemetry_hourly
WITH (timescaledb.continuous) AS
SELECT time_bucket('1 hour', time) AS bucket,
    device_id,
    metric,
    AVG(value) AS avg_value,
    MAX(value) AS max_value,
    MIN(value) AS min_value,
    STDDEV(value) AS stddev_value,
    COUNT(*) AS sample_count
FROM telemetry
GROUP BY bucket, device_id, metric
WITH NO DATA;

SELECT add_continuous_aggregate_policy('telemetry_hourly',
    start_offset => INTERVAL '1 day',
    end_offset => INTERVAL '1 hour',
    schedule_interval => INTERVAL '1 hour');
```

### E.3.3 Queries de Ejemplo

```
-- Telemetría reciente de un dispositivo (últimos 15 min)
SELECT time, metric, value, unit
FROM telemetry
WHERE device_id = 'meter_001'
    AND time > NOW() - INTERVAL '15 minutes'
ORDER BY time DESC;

-- Consumo energético diario agregado
SELECT time_bucket('1 day', time) AS day,
    device_id,
    MAX(value) - MIN(value) AS daily_energy_kwh
FROM telemetry
WHERE metric = 'energy_kwh'
    AND time > NOW() - INTERVAL '30 days'
GROUP BY day, device_id
ORDER BY day DESC;

-- Potencia promedio por hora (usando continuous aggregate)
SELECT bucket AS hour,
    device_id,
    avg_value AS avg_power_w,
    max_value AS peak_power_w
```

```

FROM telemetry_hourly
WHERE metric = 'power_w'
    AND bucket > NOW() - INTERVAL '7 days'
ORDER BY bucket DESC, device_id;

-- Alertas: voltaje fuera de rango (207-242V, RETIE Colombia)
SELECT time, device_id, value AS voltage_v
FROM telemetry
WHERE metric = 'voltage_v'
    AND time > NOW() - INTERVAL '1 hour'
    AND (value < 207.0 OR value > 242.0)
ORDER BY time DESC;

-- Dispositivos con mayor consumo (últimas 24h)
SELECT device_id,
       MAX(value) - MIN(value) AS energy_consumed_kwh
FROM telemetry
WHERE metric = 'energy_kwh'
    AND time > NOW() - INTERVAL '24 hours'
GROUP BY device_id
ORDER BY energy_consumed_kwh DESC
LIMIT 10;

```

### E.3.4 Mantenimiento

```

-- Ver tamaño de hypertables y chunks
SELECT hypertable_name,
       pg_size.pretty(hypertable_size(format('%I.%I', hypertable_schema, hypertable_name))) AS size
FROM timescaledb_information.hypertables
ORDER BY hypertable_size(format('%I.%I', hypertable_schema, hypertable_name)) DESC;

-- Ver chunks comprimidos
SELECT chunk_schema, chunk_name,
       pg_size.pretty(before_compression_total_bytes) AS before,
       pg_size.pretty(after_compression_total_bytes) AS after,
       round((1 - after_compression_total_bytes::numeric / before_compression_total_bytes::numeric) * 100) AS compression_ratio
FROM timescaledb_information.compressed_chunk_stats
ORDER BY before_compression_total_bytes DESC;

-- Forzar compresión manual de chunks antiguos
SELECT compress_chunk(i)
FROM show_chunks('telemetry', older_than => INTERVAL '7 days') i;

-- Actualizar estadísticas para optimizador de queries
ANALYZE telemetry;
ANALYZE telemetry_15min;
ANALYZE telemetry_hourly;

-- Vacuuming manual (liberar espacio)
VACUUM ANALYZE telemetry;

```

## E.4 Generación de Certificados X.509 para mTLS

### E.4.1 Autoridad Certificadora (CA)

```
#!/bin/bash
# Crear CA para IEEE 2030.5 mTLS

# CA privada
openssl ecparam -name prime256v1 -genkey -noout -out ca.key
chmod 600 ca.key

# Certificado CA (válido 10 años)
openssl req -new -x509 -sha256 -key ca.key -out ca.crt -days 3650 \
-subj "/C=C0/ST=Antioquia/L=Medellin/O=SmartGrid CA/CN=SmartGrid Root CA"

# Verificar CA
openssl x509 -in ca.crt -text -noout
```

### E.4.2 Certificado Servidor IEEE 2030.5

```
# Key privada servidor
openssl ecparam -name prime256v1 -genkey -noout -out server.key

# CSR (Certificate Signing Request)
openssl req -new -sha256 -key server.key -out server.csr \
-subj "/C=C0/ST=Antioquia/L=Medellin/O=SmartGrid/CN=gateway.local"

# Extensiones SAN (Subject Alternative Name)
cat > server_ext.cnf <<EOF
subjectAltName = DNS:gateway.local,DNS:*.gateway.local,IP:192.168.1.1
extendedKeyUsage = serverAuth
EOF

# Firmar con CA (válido 2 años)
openssl x509 -req -sha256 -in server.csr -CA ca.crt -CAkey ca.key \
-CAcreateserial -out server.crt -days 730 -extfile server_ext.cnf

# Verificar cadena
openssl verify -CAfile ca.crt server.crt
```

### E.4.3 Certificado Cliente SEP 2.0

```
# Key privada cliente
```

```
openssl ecparam -name prime256v1 -genkey -noout -out client.key

# CSR cliente
openssl req -new -sha256 -key client.key -out client.csr \
-subj "/C=C0/ST=Antioquia/L=Medellin/O=SmartGrid/CN=meter001"

# Extensiones cliente
cat > client_ext.cnf <<EOF
extendedKeyUsage = clientAuth
EOF

# Firmar con CA
openssl x509 -req -sha256 -in client.csr -CA ca.crt -CAkey ca.key \
-CAcreateserial -out client.crt -days 730 -extfile client_ext.cnf

# LFDI (Long Form Device Identifier) = SHA256 del certificado
openssl x509 -in client.crt -outform DER | openssl dgst -sha256 -binary | xxd -p -c 32
```

#### E.4.4 Prueba mTLS

```
# Curl con autenticación mutua
curl -v --cacert ca.crt --cert client.crt --key client.key \
https://gateway.local:8883/dcap

# OpenSSL s_client test
openssl s_client -connect gateway.local:8883 \
-CAfile ca.crt -cert client.crt -key client.key \
-showcerts
```

# F Anexo E: Implementación Nodo IoT de Referencia

Este anexo documenta la implementación de referencia de un nodo IoT sensor basado en ESP32-C6, utilizando el protocolo LwM2M (Lightweight M2M) sobre Thread, con integración a ThingsBoard Edge vía el gateway. El código fuente completo está disponible en el repositorio [jsebgiraldo/Tesis-app](https://github.com/jsebgiraldo/Tesis-app) en la ruta `projects/lwm2m/esp-idf/thingsboard_lwm2m_temperature_humidity`.

## F.1 Arquitectura del Nodo

### F.1.1 Hardware

- **MCU:** ESP32-C6 (RISC-V, 160 MHz, 512 KB SRAM)
- **Radio:** IEEE 802.15.4 (Thread 1.3) integrado
- **Sensores:** DHT22 simulado (temperatura/humedad)
- **Alimentación:** Batería Li-Ion 18650 3.7V + regulador 3.3V
- **Modos de bajo consumo:** Deep sleep (<20 µA), light sleep ( 800 µA)

### F.1.2 Stack de Software

- **Framework:** ESP-IDF 5.1+ (FreeRTOS)
- **Pila Thread:** OpenThread (Joiner commissioning)
- **Pila LwM2M:** AVSystems Anjay 3.x (cliente LwM2M 1.1)
- **Objetos IPSO:** Temperature (3303), Humidity (3304)
- **Objetos LwM2M:** Device (3), Connectivity Monitoring (4), Location (6)

- **Transporte:** CoAP sobre UDP/IPv6 (Thread)

## F.2 Código Principal

### F.2.1 main.c

Punto de entrada de la aplicación con inicialización de subsistemas:

```
#include <stdio.h>
#include "freertos/FreeRTOS.h"
#include "freertos/task.h"
#include "esp_log.h"
#include "nvs_flash.h"
#include "esp_sleep.h"
#include "driver/gpio.h"

// Módulos locales
#include "wifi_provisioning.h"
#include "thread_prov.h"
#include "led_status.h"

void lwm2m_client_start(void);

static const char *TAG = "lwm2m_main";

// GPIO para botón de factory reset (ESP32-C6: GPIO9 típico)
#define CONFIG_BOARD_BOOT_BUTTON_GPIO 9
#define CONFIG_FACTORY_RESET_HOLD_MS 5000

static inline bool is_deep_sleep_wake_capable_gpio(gpio_num_t gpio)
{
    // En ESP32-C6, GPIO0-GPIO7 son LP GPIOs (wake from deep sleep)
    return (gpio >= GPIO_NUM_0 && gpio <= GPIO_NUM_7);
}

static void factory_reset_task(void* arg)
{
    const gpio_num_t btn = (gpio_num_t)CONFIG_BOARD_BOOT_BUTTON_GPIO;
    const TickType_t hold_ticks = pdMS_TO_TICKS(CONFIG_FACTORY_RESET_HOLD_MS);

    gpio_config_t io_conf = {
        .pin_bit_mask = (1ULL << btn),
        .mode = GPIO_MODE_INPUT,
        .pull_up_en = GPIO_PULLUP_ENABLE,
        .pull_down_en = GPIO_PULLDOWN_DISABLE,
        .intr_type = GPIO_INTR_DISABLE
    }
}
```

```

};

gpio_config(&io_conf);

while (1) {
    if (gpio_get_level(btn) == 0) { // Botón presionado (activo bajo)
        TickType_t press_start = xTaskGetTickCount();

        while (gpio_get_level(btn) == 0) {
            TickType_t elapsed = xTaskGetTickCount() - press_start;
            if (elapsed >= hold_ticks) {
                ESP_LOGW(TAG, "Factory reset triggered! Erasing NVS...");

                // Parpadeo LED rápido para indicar reset
                led_status_factory_reset();

                // Borrar partición NVS
                nvs_flash_erase();
                nvs_flash_init();

                ESP_LOGW(TAG, "Factory reset complete. Rebooting...");
                vTaskDelay(pdMS_TO_TICKS(1000));
                esp_restart();
            }
            vTaskDelay(pdMS_TO_TICKS(100));
        }
    }
    vTaskDelay(pdMS_TO_TICKS(200));
}

void app_main(void)
{
    ESP_LOGI(TAG, "==== LwM2M Temperature/Humidity Node ===");
    ESP_LOGI(TAG, "ESP-IDF version: %s", esp_get_idf_version());

    // Inicializar NVS (almacenamiento persistente)
    esp_err_t ret = nvs_flash_init();
    if (ret == ESP_ERR_NVS_NO_FREE_PAGES ||
        ret == ESP_ERR_NVS_NEW_VERSION_FOUND) {
        ESP_ERROR_CHECK(nvs_flash_erase());
        ret = nvs_flash_init();
    }
    ESP_ERROR_CHECK(ret);

    // Inicializar LED de estado
    led_status_init();
    led_status_set(LED_STATUS_BOOTING);

    // Iniciar tarea de factory reset en background
    xTaskCreate(factory_reset_task, "factory_rst", 2048, NULL,
               tskIDLE_PRIORITY + 1, NULL);

#if CONFIG_LWM2M_NETWORK_USE_THREAD
    ESP_LOGI(TAG, "Starting Thread Provisioning...");

```

```

thread_provisioning_init();

ESP_LOGI(TAG, "Waiting for Thread network attachment...");
thread_provisioning_wait_connected();

ESP_LOGI(TAG, "Thread connected! Starting LwM2M client...");
led_status_set(LED_STATUS_CONNECTED);
lwm2m_client_start();

#elif CONFIG_LWM2M_NETWORK_USE_WIFI
ESP_LOGI(TAG, "Starting WiFi Provisioning...");
wifi_provisioning_init();

ESP_LOGI(TAG, "Waiting for WiFi connection...");
wifi_provisioning_wait_connected();

ESP_LOGI(TAG, "WiFi connected! Starting LwM2M client...");
led_status_set(LED_STATUS_CONNECTED);
lwm2m_client_start();

#else
ESP_LOGE(TAG, "No network backend enabled. "
          "Enable Thread or WiFi in menuconfig.");
led_status_set(LED_STATUS_ERROR);
#endif
}

```

## F.3 Cliente LwM2M

### F.3.1 lwm2m\_client.c (fragmento principal)

Cliente Anjay con registro de objetos IPSO y manejo de eventos:

```

#include "sdkconfig.h"
#include "freertos/FreeRTOS.h"
#include "freertos/task.h"
#include "esp_log.h"
#include "esp_event.h"
#include "esp_system.h"
#include "esp_wifi.h"
#include "esp_netif.h"
#include <string.h>
#include <stdlib.h>

// Objetos LwM2M
#include "device_object.h"

```

```

#include "firmware_update.h"
#include "temp_object.h"
#include "humidity_object.h"
#include "onoff_object.h"
#include "connectivity_object.h"
#include "location_object.h"

// AVSystems Anjay
#include <anjay/anjay.h>
#include <anjay/security.h>
#include <anjay/server.h>
#include <avsystem/commons/avs_time.h>
#include <avsystem/commons/avs_log.h>

static const char *TAG = "lwm2m_client";

// Endpoint name (único por dispositivo, basado en MAC)
static char g_endpoint_name[32] = {0};

static void resolve_endpoint_name(void)
{
    if (strlen(g_endpoint_name) > 0) {
        return; // Ya resuelto
    }

#ifdef CONFIG_LWM2M_ENDPOINT_NAME
    strncpy(g_endpoint_name, CONFIG_LWM2M_ENDPOINT_NAME,
            sizeof(g_endpoint_name) - 1);
#else
    // Generar desde MAC address
    uint8_t mac[6];
    esp_efuse_mac_get_default(mac);
    snprintf(g_endpoint_name, sizeof(g_endpoint_name),
             "esp32c6_%02x%02x%02x", mac[3], mac[4], mac[5]);
#endif
}

static int setup_security(anjay_t *anjay)
{
    // Servidor LwM2M (ThingsBoard Edge en gateway Thread)
    const anjay_security_instance_t security = {
        .ssid = 123, // Server Short ID
        .server_uri = CONFIG_LWM2M_SERVER_URI, // coap://[fd00::1]:5683
        .security_mode = ANJAY_SECURITY_NOSEC, // Sin DTLS (red Thread confiable)
        .bootstrap_server = false
    };

    anjay_iid_t security_iid = ANJAY_ID_INVALID;
    int result = anjay_security_object_add_instance(anjay, &security,
                                                    &security_iid);
    if (result) {
        ESP_LOGE(TAG, "Failed to add Security instance: %d", result);
        return result;
    }
}

```

```

ESP_LOGI(TAG, "Security object configured: URI=%s SSID=%d",
         security.server_uri, security.ssid);
return 0;
}

static int setup_server(anjay_t *anjay)
{
    const anjay_server_instance_t server = {
        .ssid = 123,
        .lifetime = 300,           // 5 min
        .default_min_period = 1,   // Notificaciones: mín 1s
        .default_max_period = -1,  // Servidor define máximo
        .disable_timeout = -1,
        .binding = "U"            // UDP
    };

    anjay_iid_t server_iid = ANJAY_ID_INVALID;
    int result = anjay_server_object_add_instance(anjay, &server,
                                                &server_iid);
    if (result) {
        ESP_LOGE(TAG, "Failed to add Server instance: %d", result);
        return result;
    }

    ESP_LOGI(TAG, "Server object configured: Lifetime=%ds Binding=%s",
             server.lifetime, server.binding);
    return 0;
}

static void lwm2m_client_task(void *arg)
{
    avs_log_set_default_level(AVS_LOG_DEBUG);

    const anjay_dm_object_def_t **dev_obj = NULL;
    const anjay_dm_object_def_t **loc_obj = NULL;

    resolve_endpoint_name();
    ESP_LOGI(TAG, "LwM2M Endpoint: %s", g_endpoint_name);

    // Configuración Anjay
    anjay_configuration_t cfg = {
        .endpoint_name = g_endpoint_name,
        .in_buffer_size = CONFIG_LWM2M_IN_BUFFER_SIZE, // 4096
        .out_buffer_size = CONFIG_LWM2M_OUT_BUFFER_SIZE, // 4096
        .msg_cache_size = CONFIG_LWM2M_MSG_CACHE_SIZE, // 4096
    };

#define ANJAY_WITH_LWM2M11
// Forzar LwM2M 1.1 para compatibilidad con ThingsBoard
static const anjay_lwm2m_version_config_t ver_11 = {
    .minimum_version = ANJAY_LWM2M_VERSION_1_1,
    .maximum_version = ANJAY_LWM2M_VERSION_1_1
};

```

```

cfg.lwm2m_version_config = &ver_11;
#endif

anjay_t *anjay = anjay_new(&cfg);
if (!anjay) {
    ESP_LOGE(TAG, "Could not create Anjay instance");
    vTaskDelete(NULL);
}

// Instalar objetos Security/Server
if (anjay_security_object_install(anjay) ||
    anjay_server_object_install(anjay)) {
    ESP_LOGE(TAG, "Could not install Security/Server objects");
    goto cleanup;
}

if (setup_security(anjay) || setup_server(anjay)) {
    goto cleanup;
}

// Registrar objetos IPSO
if (anjay_register_object(anjay, temp_object_def())) {
    ESP_LOGE(TAG, "Could not register Temperature (3303)");
    goto cleanup;
}

if (anjay_register_object(anjay, humidity_object_def())) {
    ESP_LOGE(TAG, "Could not register Humidity (3304)");
    goto cleanup;
}

if (anjay_register_object(anjay, connectivity_object_def())) {
    ESP_LOGE(TAG, "Could not register Connectivity (4)");
    goto cleanup;
}

// Registrar objeto Device (3)
dev_obj = device_object_create(g_endpoint_name);
if (!dev_obj || anjay_register_object(anjay, dev_obj)) {
    ESP_LOGE(TAG, "Could not register Device (3)");
    goto cleanup;
}

// Registrar objeto Location (6)
loc_obj = location_object_create();
if (!loc_obj || anjay_register_object(anjay, loc_obj)) {
    ESP_LOGE(TAG, "Could not register Location (6)");
    goto cleanup;
}

ESP_LOGI(TAG, "Starting Anjay event loop");

// Notificar objetos al servidor al inicio
anjay_notify_instances_changed(anjay, 3303); // Temperature

```

```

anjay_notify_instances_changed(anjay, 3304); // Humidity
anjay_notify_instances_changed(anjay, 4); // Connectivity

// Instalar Firmware Update (OTA)
ESP_LOGI(TAG, "Installing Firmware Update object...");
int fw_result = fw_update_install(anjay);
if (fw_result) {
    ESP_LOGW(TAG, "Firmware Update install failed: %d", fw_result);
} else {
    ESP_LOGI(TAG, "Firmware Update object ready");
}

// Loop principal
const avs_time_duration_t max_wait =
    avs_time_duration_from_scalar(100, AVS_TIME_MS);

while (1) {
    anjay_event_loop_run(anjay, max_wait);

    // Actualizar objetos cada 100ms
    device_object_update(anjay, dev_obj);
    temp_object_update(anjay);
    humidity_object_update(anjay);
    onoff_object_update(anjay);
    connectivity_object_update(anjay);
    location_object_update(anjay, loc_obj);

    // Verificar si hay OTA pendiente
    if (fw_update_requested()) {
        ESP_LOGW(TAG, "Firmware update ready, rebooting...");
        vTaskDelay(pdMS_TO_TICKS(1000));
        fw_update_reboot();
    }
}

cleanup:
    if (dev_obj) device_object_release(dev_obj);
    if (loc_obj) location_object_release(loc_obj);
    anjay_delete(anjay);
    vTaskDelete(NULL);
}

void lwm2m_client_start(void)
{
    xTaskCreate(lwm2m_client_task, "lwm2m",
                CONFIG_LWM2M_TASK_STACK_SIZE, // 8192
                NULL, tskIDLE_PRIORITY + 2, NULL);
}

```

## F.4 Objetos IPSO

### F.4.1 temp\_object.c

Implementación del objeto Temperature (3303):

```
#include "temp_object.h"
#include <math.h>
#include <stdbool.h>
#include <freertos/FreeRTOS.h>
#include <freertos/task.h>
#include <anjay/io.h>
#include <esp_log.h>

#define OID_TEMPERATURE 3303
#define IID_DEFAULT 0

// Resource IDs (según OMA SpecWorks IPSO)
#define RID_SENSOR_VALUE 5700
#define RID_SENSOR_UNITS 5701
#define RID_MIN_MEASURED 5601
#define RID_MAX_MEASURED 5602
#define RID_RESET_MIN_MAX 5605

#define TEMP_SAMPLE_INTERVAL_MS 1000
#define TEMP_DELTA_EPS 0.01f

static const char *TAG = "temp_obj";

// Estado interno
static float g_current_value = 0.0f;
static float g_min_measured = 100.0f;
static float g_max_measured = -100.0f;
static TickType_t g_last_sample_tick = 0;

static float read_temperature_sensor(void)
{
    // Simulación: senoidal 20-30°C con ruido
    TickType_t ticks = xTaskGetTickCount();
    float base = 25.0f;
    float phase = (float)(ticks % 10000) / 250.0f;
    float delta = 5.0f * sinf(phase);
    float noise = ((float)(esp_random() % 100) / 1000.0f) - 0.05f;

    return base + delta + noise;
}

static void ensure_sample(void)
{
```

```

if (g_last_sample_tick == 0) {
    float value = read_temperature_sensor();
    g_current_value = value;
    g_min_measured = value;
    g_max_measured = value;
    g_last_sample_tick = xTaskGetTickCount();

    ESP_LOGD(TAG, "init sample: value=%.3fC min=%.3f max=%.3f",
             g_current_value, g_min_measured, g_max_measured);
}
}

static int temp_list_instances(anjay_t *anjay,
                               const anjay_dm_object_def_t *const *def,
                               anjay_dm_list_ctx_t *ctx) {
(void) anjay; (void) def;
anjay_dm_emit(ctx, IID_DEFAULT);
return 0;
}

static int temp_list_resources(anjay_t *anjay,
                               const anjay_dm_object_def_t *const *def,
                               anjay_iid_t iid,
                               anjay_dm_resource_list_ctx_t *ctx) {
(void) anjay; (void) def; (void) iid;
anjay_dm_emit_res(ctx, RID_MIN_MEASURED, ANJAY_DM_RES_R,
                  ANJAY_DM_RES_PRESENT);
anjay_dm_emit_res(ctx, RID_MAX_MEASURED, ANJAY_DM_RES_R,
                  ANJAY_DM_RES_PRESENT);
anjay_dm_emit_res(ctx, RID_RESET_MIN_MAX, ANJAY_DM_RES_E,
                  ANJAY_DM_RES_PRESENT);
anjay_dm_emit_res(ctx, RID_SENSOR_VALUE, ANJAY_DM_RES_R,
                  ANJAY_DM_RES_PRESENT);
anjay_dm_emit_res(ctx, RID_SENSOR_UNITS, ANJAY_DM_RES_R,
                  ANJAY_DM_RES_PRESENT);
return 0;
}

static int temp_read(anjay_t *anjay,
                     const anjay_dm_object_def_t *const *def,
                     anjay_iid_t iid,
                     anjay_rid_t rid,
                     anjay_riid_t riid,
                     anjay_output_ctx_t *ctx) {
(void) anjay; (void) def; (void) iid; (void) riid;
ensure_sample();

switch (rid) {
case RID_SENSOR_VALUE:
    ESP_LOGD(TAG, "read Temperature -> %.3f C", g_current_value);
    return anjay_ret_float(ctx, g_current_value);

case RID_SENSOR_UNITS:
    return anjay_ret_string(ctx, "Cel"); // Celsius
}
}

```

```

case RID_MIN_MEASURED:
    ESP_LOGD(TAG, "read Min -> %.3f C", g_min_measured);
    return anjay_ret_float(ctx, g_min_measured);

case RID_MAX_MEASURED:
    ESP_LOGD(TAG, "read Max -> %.3f C", g_max_measured);
    return anjay_ret_float(ctx, g_max_measured);

default:
    return ANJAY_ERR_METHOD_NOT_ALLOWED;
}

static int temp_execute(anjay_t *anjay,
                       const anjay_dm_object_def_t *const *def,
                       anjay_iid_t iid,
                       anjay_rid_t rid,
                       anjay_execute_ctx_t *ctx) {
(void) anjay; (void) def; (void) iid; (void) ctx;

if (rid == RID_RESET_MIN_MAX) {
    ESP_LOGI(TAG, "Resetting min/max values");
    g_min_measured = g_current_value;
    g_max_measured = g_current_value;

    // Notificar cambios al servidor
    anjay_notify_changed(anjay, OID_TEMPERATURE, IID_DEFAULT,
                         RID_MIN_MEASURED);
    anjay_notify_changed(anjay, OID_TEMPERATURE, IID_DEFAULT,
                         RID_MAX_MEASURED);
    return 0;
}

return ANJAY_ERR_METHOD_NOT_ALLOWED;
}

static const anjay_dm_object_def_t OBJ_DEF = {
    .oid = OID_TEMPERATURE,
    .version = "1.1",
    .handlers = {
        .list_instances = temp_list_instances,
        .list_resources = temp_list_resources,
        .resource_read = temp_read,
        .resource_execute = temp_execute
    }
};

static const anjay_dm_object_def_t *const OBJ_DEF_PTR = &OBJ_DEF;

const anjay_dm_object_def_t *const *temp_object_def(void) {
    ensure_sample();
    return &OBJ_DEF_PTR;
}

```

```

void temp_object_update(anjay_t *anjay) {
    if (!anjay) {
        return;
    }

    TickType_t now = xTaskGetTickCount();
    if (g_last_sample_tick == 0 || (now - g_last_sample_tick) >= pdMS_TO_TICKS(TEMP_SAMPLE_INTERVAL_MS)) {

        g_last_sample_tick = now;
        bool min_changed = false;
        bool max_changed = false;

        float new_value = read_temperature_sensor();

        // Actualizar min/max
        if (new_value < g_min_measured) {
            g_min_measured = new_value;
            min_changed = true;
        }
        if (new_value > g_max_measured) {
            g_max_measured = new_value;
            max_changed = true;
        }

        // Solo notificar si cambió significativamente
        if (fabsf(new_value - g_current_value) > TEMP_DELTA_EPS) {
            ESP_LOGD(TAG, "Temperature changed: %.3f -> %.3f C",
                    g_current_value, new_value);
            g_current_value = new_value;
            anjay_notify_changed(anjay, OID_TEMPERATURE, IID_DEFAULT,
                                RID_SENSOR_VALUE);
        }

        if (min_changed) {
            anjay_notify_changed(anjay, OID_TEMPERATURE, IID_DEFAULT,
                                RID_MIN_MEASURED);
        }
        if (max_changed) {
            anjay_notify_changed(anjay, OID_TEMPERATURE, IID_DEFAULT,
                                RID_MAX_MEASURED);
        }
    }
}

```

#### F.4.2 humidity\_object.c

Implementación del objeto Humidity (3304), análogo a Temperature:

```

#include "humidity_object.h"
#include <math.h>
#include <stdbool.h>
#include <freertos/FreeRTOS.h>
#include <freertos/task.h>
#include <anjay/io.h>
#include <esp_log.h>

#define OID_HUMIDITY 3304
#define IID_DEFAULT 0
#define RID_SENSOR_VALUE 5700
#define RID_SENSOR_UNITS 5701
#define RID_MIN_MEASURED 5601
#define RID_MAX_MEASURED 5602
#define RID_RESET_MIN_MAX 5605

#define HUM_SAMPLE_INTERVAL_MS 1000
#define HUM_DELTA_EPS 0.01f

static const char *TAG = "humid_obj";

static float g_current_value = 0.0f;
static float g_min_measured = 100.0f;
static float g_max_measured = 0.0f;
static TickType_t g_last_sample_tick = 0;

static float read_humidity_sensor(void)
{
    // Simulación: senoidal 45-75%RH
    TickType_t ticks = xTaskGetTickCount();
    float base = 55.0f;
    float phase = (float)(ticks % 12000) / 300.0f;
    float delta = 10.0f * sinf(phase);
    float noise = ((float)(esp_random() % 100) / 1000.0f) - 0.05f;

    float value = base + delta + noise;

    // Clamp 0-100%
    if (value < 0.0f) value = 0.0f;
    if (value > 100.0f) value = 100.0f;

    return value;
}

// [Resto de funciones similar a temp_object.c]
// list_instances, list_resources, resource_read, resource_execute
// con lógica adaptada para humedad

static const anjay_dm_object_def_t OBJ_DEF = {
    .oid = OID_HUMIDITY,
    .version = "1.1",
    .handlers = {
        .list_instances = hum_list_instances,
        .list_resources = hum_list_resources,

```

```

    .resource_read = hum_read,
    .resource_execute = hum_execute
}
};

// Implementaciones análogas...

```

## F.5 Objetos LwM2M Core

### F.5.1 device\_object.c (fragmento)

Objeto Device (3) con métricas del dispositivo:

```

#include "device_object.h"
#include "sdkconfig.h"
#include <anjay/anjay.h>
#include <anjay/io.h>
#include <esp_system.h>
#include <esp_log.h>
#include <esp_heap_caps.h>
#include <esp_idf_version.h>

#define RID_MANUFACTURER 0
#define RID_MODEL_NUMBER 1
#define RID_SERIAL_NUMBER 2
#define RID_FIRMWARE_VERSION 3
#define RID_REBOOT 4
#define RID_BATTERY_LEVEL 9
#define RID_MEMORY_FREE 10
#define RID_ERROR_CODE 11
#define RID_CURRENT_TIME 13

#define DEVICE_MANUFACTURER "Universidad Nacional"
#define DEVICE_MODEL "ESP32-C6 LwM2M Node"
#define DEVICE_TYPE "Temperature/Humidity Sensor"

static const char *TAG = "device_obj";

typedef struct {
    const anjay_dm_object_def_t *def;
    char serial_number[32];
    int32_t battery_level;
    int32_t power_voltage_mv;
    int32_t power_current_ma;
    TickType_t last_update_tick;
    bool do_reboot;
}
```

```

} device_object_t;

static int resource_read(anjay_t *anjay,
                        const anjay_dm_object_def_t *const *obj_ptr,
                        anjay_iid_t iid,
                        anjay_rid_t rid,
                        anjay_riid_t riid,
                        anjay_output_ctx_t *ctx) {
device_object_t *obj = get_obj(obj_ptr);

switch (rid) {
case RID_MANUFACTURER:
    return anjay_ret_string(ctx, DEVICE_MANUFACTURER);

case RID_MODEL_NUMBER:
    return anjay_ret_string(ctx, DEVICE_MODEL);

case RID_SERIAL_NUMBER:
    return anjay_ret_string(ctx, obj->serial_number);

case RID_FIRMWARE_VERSION:
    return anjay_ret_string(ctx, esp_get_idf_version());

case RID_BATTERY_LEVEL:
    return anjay_ret_i32(ctx, obj->battery_level);

case RID_MEMORY_FREE:
    return anjay_ret_i32(ctx, (int32_t)esp_get_free_heap_size());

case RID_CURRENT_TIME:
    return anjay_ret_i64(ctx, (int64_t)time(NULL));

default:
    return ANJAY_ERR_NOT_FOUND;
}

static int resource_execute(anjay_t *anjay,
                           const anjay_dm_object_def_t *const *obj_ptr,
                           anjay_iid_t iid,
                           anjay_rid_t rid,
                           anjay_execute_ctx_t *ctx) {
device_object_t *obj = get_obj(obj_ptr);

if (rid == RID_REBOOT) {
    ESP_LOGW(TAG, "Reboot requested via LwM2M");
    obj->do_reboot = true;
    return 0;
}

return ANJAY_ERR_METHOD_NOT_ALLOWED;
}

void device_object_update(anjay_t *anjay,

```

```

        const anjay_dm_object_def_t *const *def) {
device_object_t *obj = get_obj(def);

if (obj->do_reboot) {
    ESP_LOGW(TAG, "Rebooting...");
    esp_restart();
}

// Actualizar nivel de batería simulado cada 10s
TickType_t now = xTaskGetTickCount();
if ((now - obj->last_update_tick) >= pdMS_TO_TICKS(10000)) {
    obj->last_update_tick = now;

    // Simulación: batería 70-100% con lenta descarga
    obj->battery_level -= 1;
    if (obj->battery_level < 70) obj->battery_level = 100;

    anjay_notify_changed(anjay, 3, 0, RID_BATTERY_LEVEL);
}
}

```

## F.6 Conectividad Thread

### F.6.1 thread\_prov.c (fragmento)

Provisioning de red Thread con OpenThread Joiner:

```

#include "thread_prov.h"
#include <string.h>
#include <esp_log.h>
#include <esp_openthread.h>
#include <esp_openthread_lock.h>
#include <openthread/thread.h>
#include <openthread/joiner.h>

static const char *TAG = "thread_prov";

static void ot_joiner_callback(otError error, void *context)
{
    if (error == OT_ERROR_NONE) {
        ESP_LOGI(TAG, "Joiner success! Attached to Thread network");

        esp_openthread_lock_acquire(portMAX_DELAY);
        otThreadSetEnabled(esp_openthread_get_instance(), true);
        esp_openthread_lock_release();
    } else {

```

```

        ESP_LOGE(TAG, "Joiner failed: %d", error);
    }
}

void thread_provisioning_init(void)
{
    ESP_LOGI(TAG, "Initializing OpenThread...");

    // Configuración Thread por defecto
    esp_openthread_platform_config_t config = {
        .radio_config = ESP_OPENTHREAD_DEFAULT_RADIO_CONFIG(),
        .host_config = ESP_OPENTHREAD_DEFAULT_HOST_CONFIG(),
        .port_config = ESP_OPENTHREAD_DEFAULT_PORT_CONFIG(),
    };

    ESP_ERROR_CHECK(esp_openthread_init(&config));

    otInstance *instance = esp_openthread_get_instance();

    // Iniciar Joiner con PSKd (pre-shared key for device)
    esp_openthread_lock_acquire(portMAX_DELAY);

    const char *pskd = CONFIG_THREAD_JOINER_PSKD; // "JO1NME"
    otError error = otJoinerStart(instance, pskd, NULL, PACKAGE_NAME,
                                  NULL, NULL, NULL,
                                  ot_joiner_callback, NULL);

    esp_openthread_lock_release();

    if (error != OT_ERROR_NONE) {
        ESP_LOGE(TAG, "Failed to start Joiner: %d", error);
    } else {
        ESP_LOGI(TAG, "Joiner started with PSKd");
    }
}

void thread_provisioning_wait_connected(void)
{
    ESP_LOGI(TAG, "Waiting for Thread attachment...");

    while (1) {
        esp_openthread_lock_acquire(portMAX_DELAY);
        otInstance *instance = esp_openthread_get_instance();
        otDeviceRole role = otThreadGetDeviceRole(instance);
        esp_openthread_lock_release();

        if (role >= OT_DEVICE_ROLE_CHILD) {
            ESP_LOGI(TAG, "Thread attached! Role: %d", role);
            break;
        }

        vTaskDelay(pdMS_TO_TICKS(1000));
    }
}

```

## F.7 CMakeLists.txt

### F.7.1 Configuración de Build

```

idf_component_register(
    SRCS
        "main.c"
        "lwm2m_client.c"
        "device_object.c"
        "temp_object.c"
        "humidity_object.c"
        "onoff_object.c"
        "connectivity_object.c"
        "firmware_update.c"
        "location_object.c"
        "wifi_provisioning.c"
        "thread_prov.c"
        "led_status.c"

    INCLUDE_DIRS
        "."
        "${IDF_PATH}/components/app_update/include"

    REQUIRES
        freertos
        esp_netif
        esp_wifi
        nvs_flash
        lwip
        anjay-esp-idf
        wifi_provisioning
        openthread
        driver
        app_update
        led_strip

    PRIV_REQUIRES
        app_update
)

# Asegurar headers app_update visibles
target_include_directories(${COMPONENT_LIB} PRIVATE
    "${IDF_PATH}/components/app_update/include")

```

## F.8 sdkconfig.defaults

### F.8.1 Configuración por Defecto

```

# LwM2M Server URI (gateway Thread border router)
CONFIG_LWM2M_SERVER_URI="coap://[fd00::1]:5683"
CONFIG_LWM2M_ENDPOINT_NAME="esp32c6_tempid"

# Buffer sizes
CONFIG_LWM2M_IN_BUFFER_SIZE=4096
CONFIG_LWM2M_OUT_BUFFER_SIZE=4096
CONFIG_LWM2M_MSG_CACHE_SIZE=4096
CONFIG_LWM2M_TASK_STACK_SIZE=8192

# Thread Joiner
CONFIG_LWM2M_NETWORK_USE_THREAD=y
CONFIG_THREAD_JOINER_PSKD="JO1NME"

# OpenThread
CONFIG_OPENTHREAD_ENABLED=y
CONFIG_OPENTHREAD_COMMISSIONER=n
CONFIG_OPENTHREAD_JOINER=y
CONFIG_OPENTHREAD_NETWORK_NAME="SmartGrid-Thread"
CONFIG_OPENTHREAD_NETWORK_CHANNEL=15
CONFIG_OPENTHREAD_NETWORK_PANID=0x1234
CONFIG_OPENTHREAD_NETWORK_EXTPANID="1111111122222222"

# Anjay
CONFIG_ANJAY_WITH_ATTR_STORAGE=y
CONFIG_ANJAY_WITH_LWM2M11=y

# FreeRTOS
CONFIG_FREERTOS_HZ=1000
CONFIG_FREERTOS_UNICORE=n

# ESP32-C6
CONFIG_ESP_DEFAULT_CPU_FREQ_MHZ_160=y
CONFIG_ESP_PHY_RF_CAL_FULL=y

# Power Management
CONFIG_PM_ENABLE=y
CONFIG_PM_DFS_INIT_AUTO=y
CONFIG_PM_POWER_DOWN_CPU_IN_LIGHT_SLEEP=y
CONFIG_PM_POWER_DOWN_PERIPHERAL_IN_LIGHT_SLEEP=y

# Logging
CONFIG_LOG_DEFAULT_LEVEL_INFO=y
CONFIG_LOG_MAXIMUM_LEVEL_DEBUG=y

```

## F.9 Uso del Nodo

### F.9.1 Compilación y Flash

```
# Desde directorio del proyecto
cd projects/lwm2m/esp-idf/thingsboard_lwm2m_temperature_humidity

# Configurar (opcional, solo primera vez)
idf.py menuconfig

# Compilar
idf.py build

# Flash al ESP32-C6
idf.py -p COM3 flash monitor # Windows
idf.py -p /dev/ttyUSB0 flash monitor # Linux

# Solo monitor
idf.py -p COM3 monitor
```

### F.9.2 Comisionamiento Thread

En el gateway OTBR:

```
# Habilitar comisionado
docker exec -it otbr ot-ctl commissioner start
docker exec -it otbr ot-ctl commissioner joiner add * JOINME

# Verificar dispositivo unido
docker exec -it otbr ot-ctl child table
# Output esperado: Child ID | RLOC16 | Timeout | ... | IPv6 Address
```

### F.9.3 Verificación LwM2M

En ThingsBoard Edge:

1. Navegar a *Devices* → se debe crear automáticamente `esp32c6_xxxxxx`
2. *Latest Telemetry* mostrará: temperature, humidity, battery\_level, memory\_free
3. *Attributes* mostrará: manufacturer, model, fw\_version

4. Configurar *Observe* en recursos 3303/0/5700 y 3304/0/5700 para notificaciones automáticas

# Referencias Bibliográficas

**De Castro Korgi, R.**: , 2010; *El Universo La TeX*; Universidad Nacional de Colombia, Bogota DC; 2<sup>a</sup> edición; ISBN 958701060-4.

**Morse Micro**: , 2025; Morse Micro Announces Mass Production of MM8108 Wi-Fi HaLow SoC, Modules, Evaluation Kit and Ha-LowLink 2; PR Newswire; URL <https://finance.yahoo.com/news/morse-micro-announces-mass-production-070100596.html>; accessed: 2025-10-30.