friendly technologies | The IoT & Device Management Company

Future Proofing IoT Device Deployments

May 25-27, 2021

Future Proofing – The case for improvements

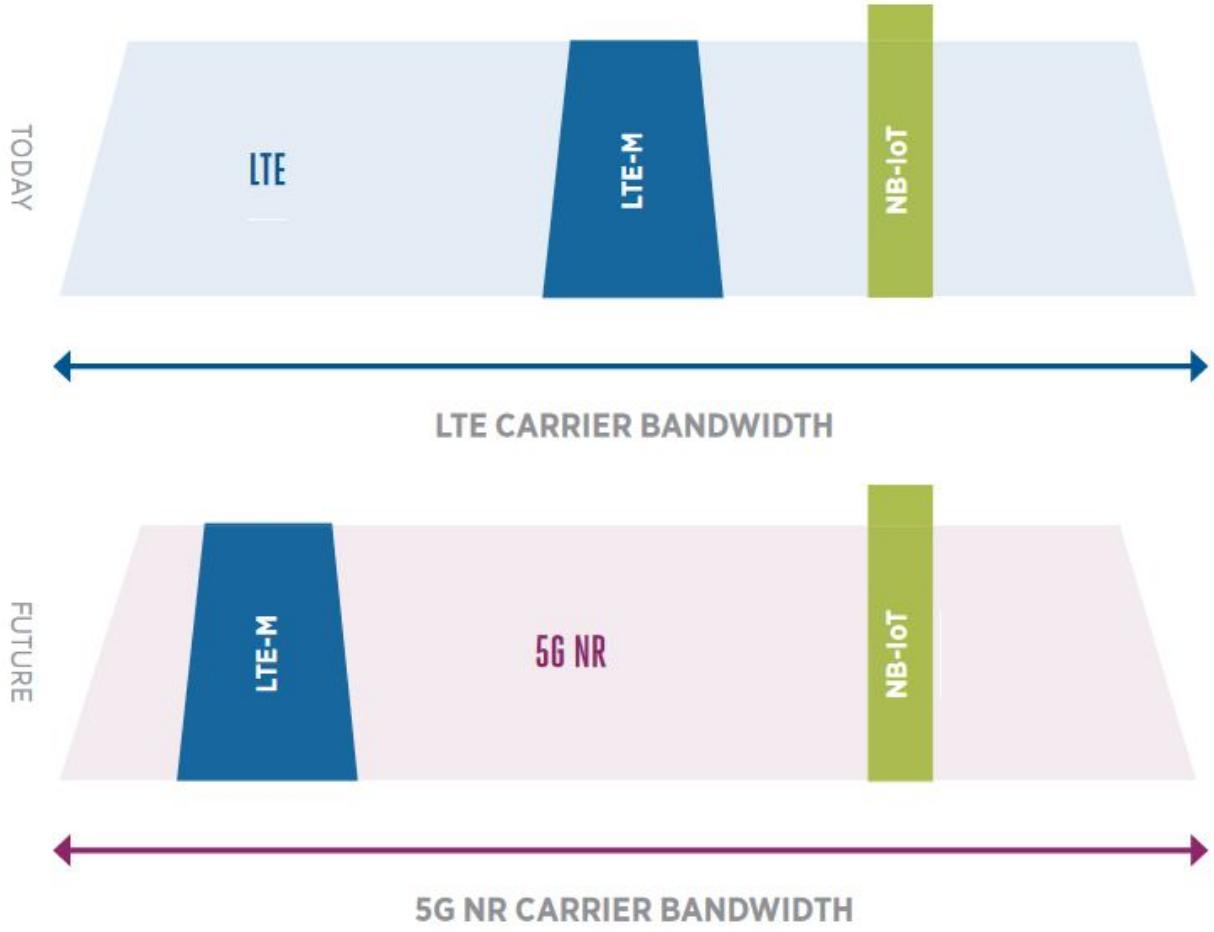
Service Providers have already invested heavily in LTE (4G) support for Low Power WAN (LPWAN), being NB-IoT and LTE-M. With the deployment of new 3GPP standards, including 5G NR, Service Providers need to ensure that their current IoT device fleet(s) are well supported, as well as the scaling for mass IoT deployments to ensure future proofing.

The following requirements arise:

- Large numbers of devices – supporting high connection densities.
- Low device cost (IP vs non-IP) – resource constrained devices (low footprint RAM, CPU, Flash, Chipsets).
- Ultra long battery life.
- Coverage in harsh environments.
- Current LPWAN devices spectrum use, to be supported in new 5G deployments.

LPWAN in 5G World

- Existing LTE (4G) spectrum resources, including LPWAN (NB-IoT & LTE-M).
- NB-IoT & LTE-M incorporated into new 5G NR spectrum.
- NB-IoT incorporates CAT-NB1 and CAT-NB2.
- LTE-M incorporates CAT-M1 and CAT-M2.



GSMA – Mobile IoT in the 5G Future – [1]

NB-IoT vs LTE-M

V·T·E [12][13]	LTE Cat 1	LTE-M				NB-IoT		EC-GSM-IoT
		LC-LTE/MTCe	eMTC					
		LTE Cat 0	LTE Cat M1	LTE Cat M2	non-BL	LTE Cat NB1	LTE Cat NB2	
3GPP Release	Release 8	Release 12	Release 13	Release 14	Release 14	Release 13	Release 14	Release 13
Downlink Peak Rate	10 Mbit/s	1 Mbit/s	1 Mbit/s	~4 Mbit/s	~4 Mbit/s	26 kbit/s	127 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	1 Mbit/s	1 Mbit/s	~7 Mbit/s	~7 Mbit/s	66 kbit/s (multi-tone) 16.9 kbit/s (single-tone)	159 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Latency	50–100 ms	not deployed	10–15 ms			1.6–10 s		700 ms – 2 s
Number of Antennas	2	1	1	1	1	1	1	1–2
Duplex Mode	Full Duplex	Full or Half Duplex	Full or Half Duplex	Full or Half Duplex	Full or Half Duplex	Half Duplex	Half Duplex	Half Duplex
Device Receive Bandwidth	1.4–20 MHz	1.4–20 MHz	1.4 MHz	5 MHz	5 MHz	180 kHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)	1 (SISO)	1 (SISO)	1 (SISO)	1 (SISO)	1 (SISO)	1 (SISO)	1–2
Device Transmit Power	23 dBm	23 dBm	20 / 23 dBm	20 / 23 dBm	20 / 23 dBm	20 / 23 dBm	14 / 20 / 23 dBm	23 / 33 dBm

ubidots – NB-IoT vs LTE-M – [2]

IoT Protocols – Future Proofing

IoT Protocols Comparison - Functions

LwM2M vs USP vs MQTT vs CoAP (Endpoint) - Functions

friendly technologies | The IoT & Device Management Company

Features	LwM2M	TR-369 USP	MQTT	CoAP
Concept	OMA LWM2M standard is open, allowing to connect resource constrained IoT devices to LPWAN networks efficiently.	BBF standard, faster and more flexible. Manage WiFi deployments, onboarding IoT LPWAN, self-care, container management, better security.	Legacy protocol, based on a publish-subscribe model, utilizing TCP connection oriented protocol. Allowing for ease of disseminating data.	Constrained Application Protocol designed to enable simple, constrained devices to join the IoT, through constrained networks, low bandwidth and low availability
Device Management	Defined and built-in Objects & Resources to perform various device management tasks, such as updating device parameters, collecting telemetry data.	Multiple management servers are allowed at the same time without restriction of location. Add, Set, Delete, Get, GetSupportedDM, GetInstances, Operate.	No defined device management functions. Topics need to be defined and are custom	No defined device management functions. Proprietary payloads are defined and operations are custom.
Provisioning	Built-in Bootstrap process, Automated Registration & Provisioning. Automated Device data discovery.	Built-in Bootstrap process, Automated Registration & Provisioning. Automated Device data discovery.	No defined Provisioning. Topics need to be defined in a proprietary way, and operations thereof.	No defined Provisioning. CoAP payloads need to be defined in a proprietary way, operations thereof.
Firmware upgrade	Built-in and defined by the LWM2M standard. Including Blockwise transfers & Delta FW upgrades.	Built-in and defined by the USP standard, including application and container management.	No defined FoTA process. Topics need to be defined in a proprietary way, and implementation thereof.	No defined FoTA. CoAP payloads need to be defined in a proprietary way, and implementation thereof.

IoT Protocols Comparison - Features

LwM2M vs USP vs MQTT vs CoAP (Endpoint) - Features

friendly technologies | The IoT & Device Management Company

Features	LwM2M	TR-369 USP	MQTT	CoAP
Transport Protocols	UDP, TCP, SMS, NIDD, LoRaWAN	TCP, UDP, XMPP	TCP	UDP
Application Layer	CoAP, MQTT	CoAP, WebSocket, MQTT, STOMP	None	CoAP
Payload	CBOR, Opaque, TLV, JSON	Protocol Buffers (binary)	Topic defined (text/binary)	CBOR, JSON or user defined
Security	DTLS, TLS, OSCORE	DTLS or TLS Controller trust establishment procedures ACL mechanism E2E application-level security/encryption	SSL/TLS	TLS
Data Management	Observe & Notify, Autonomous Notify. Data Orchestration, Cloud streaming & Cloud ready	Notify, and bulk statistics or telemetry data collection. Cloud ready	Publish & Subscribe topics	End to End proprietary
Standards	OMA, IETF	BBF, IETF	OASIS, ISO	IETF
Networking	IPV4, IPV6, and non-IP channels	IPV4, IPV6	IPV4, IPV6	IPV4, IPV6

IoT Protocols Comparison - Performance

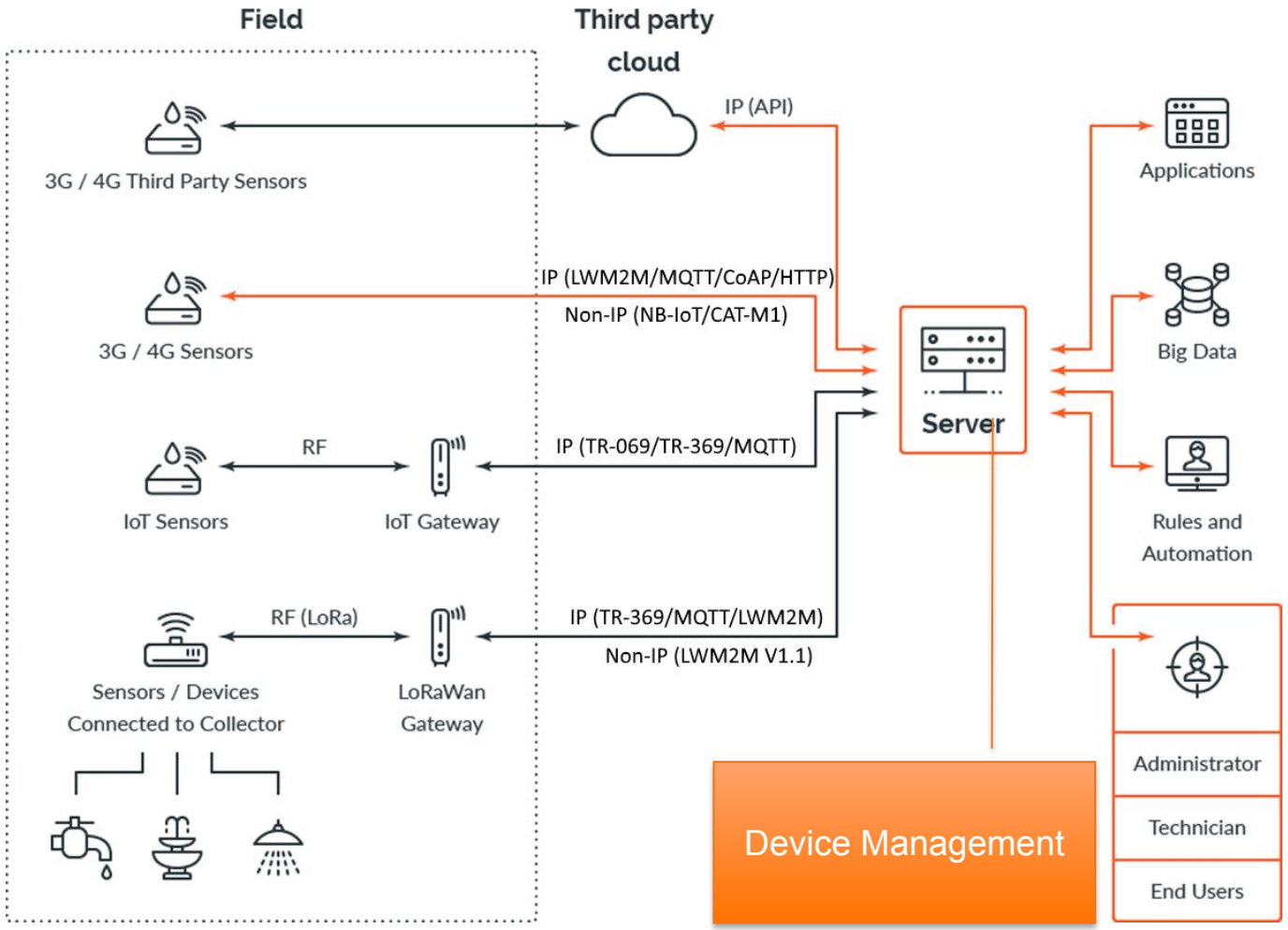
LwM2M vs USP vs MQTT vs CoAP (Endpoint) - Performance

friendly technologies | The IoT & Device Management Company

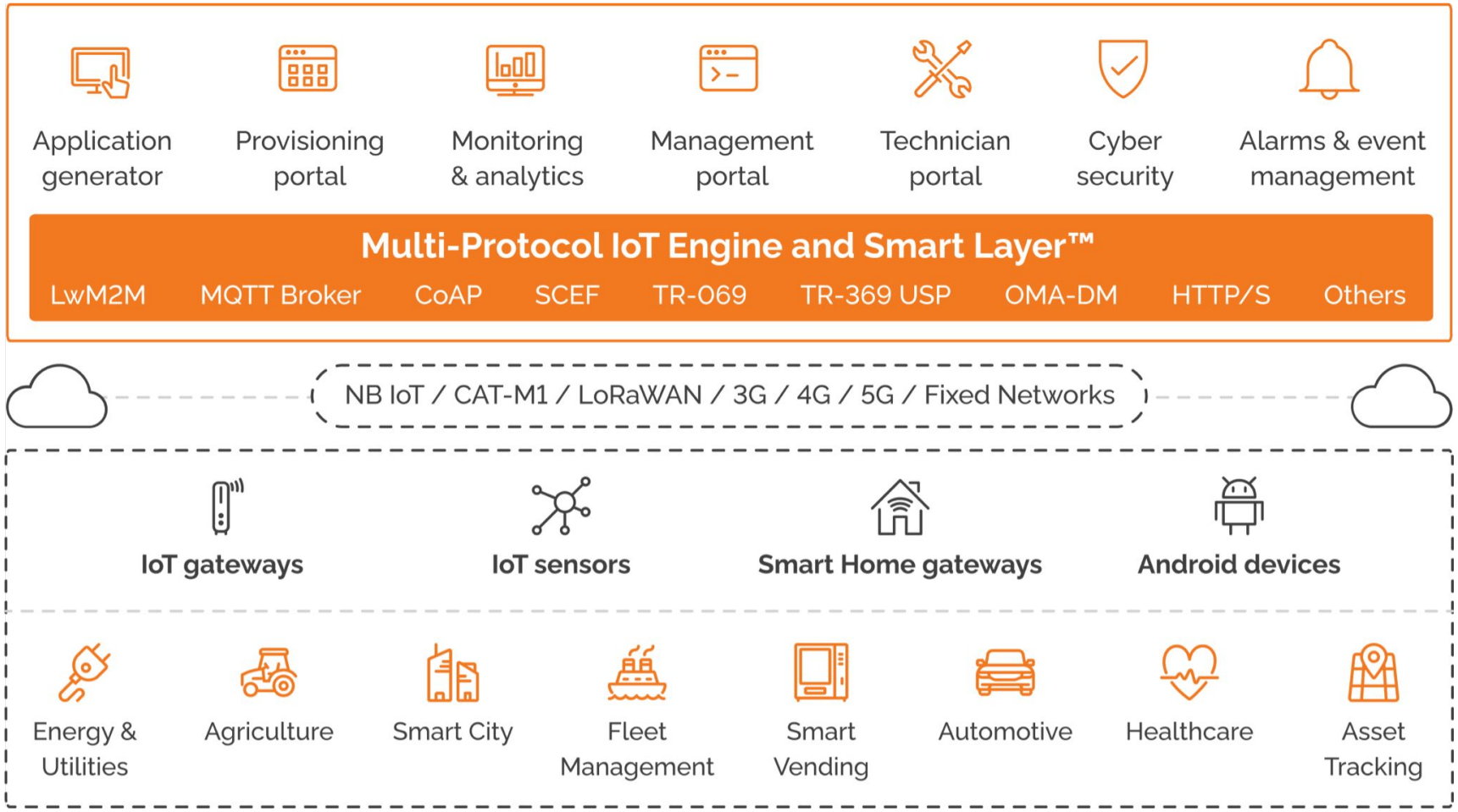
Features	LwM2M	TR-369 USP	MQTT	CoAP
Resources	Low to very low footprint	Low to Medium footprint	Medium footprint	Very low footprint
Powered Devices	Very low power consumption	Could be used for low powered devices, but excels in powered gateway type IoT devices	Medium to high power consumption	Very low power consumption
Bandwidth	Low – 88% more efficient than MQTT*	Low to Medium	Medium to High, depending on encoding	Low – in its simplest form
Scalability	Multiple Bootstrap & Registration Servers, high scalable data channels (Notify = Publish)	Multiple servers, highly scalable	Publish & Subscribe, but limited to TCP socket connections	Yes, but proprietary implementation
Reliability	High-availability, Geo-redundancy, and Clustering options for LWM2M Servers	HA, Geo-Redundancy, Clustering options for USP Servers	Need to architect a robust MQTT Broker implementation	Yes, but proprietary implementation
Investment	Low, LWM2M clients and servers off-the-shelf	Low, USP clients and servers being offered off-the-shelf now	Low, MQTT clients and brokers off-the-shelf	High, require to custom design architecture, data models, and operational functions from scratch

IoT Edge devices – Future Proofing

IoT Connectivity Architecture



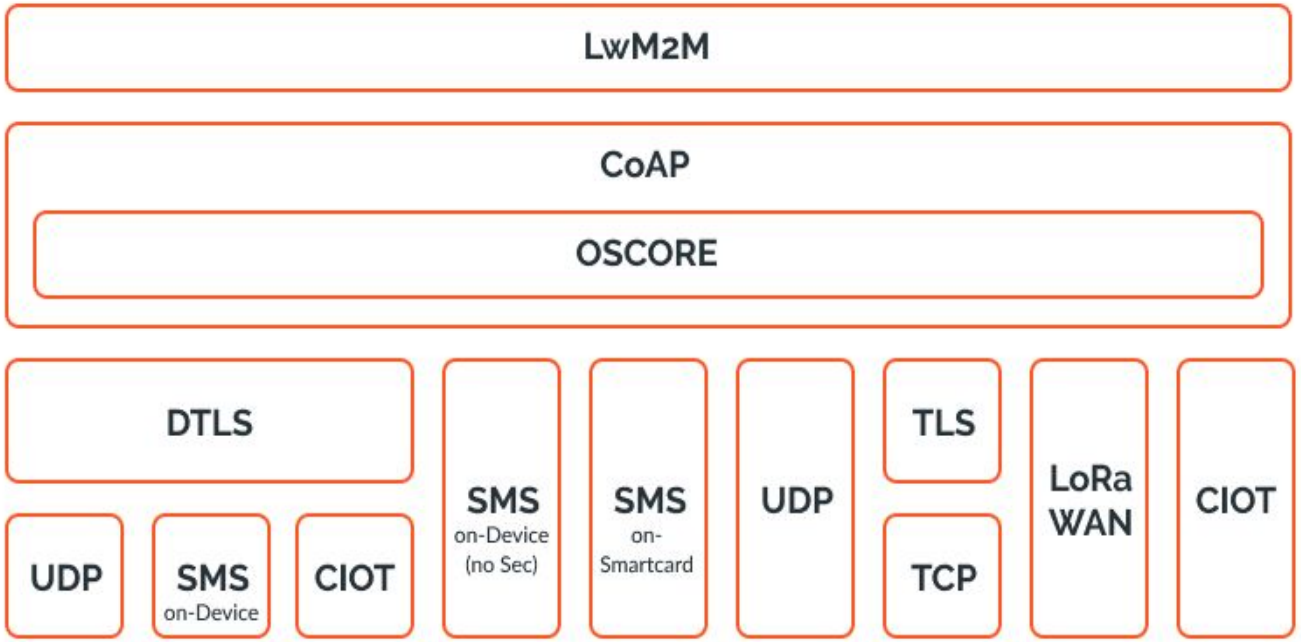
Friendly One-IoT™ Platform Modules



LwM2M IoT Device Connectivity

- OMA LwM2M V1.1/1.2 standards protocols.
- Security end-to-end from device, to connectivity to application objects.
- Bootstraps & registers LwM2M devices.
- Device sensor data ingested by Observe/Notify mechanism.
- Various Object/Resources for sensor data.
- Multiple access technologies.

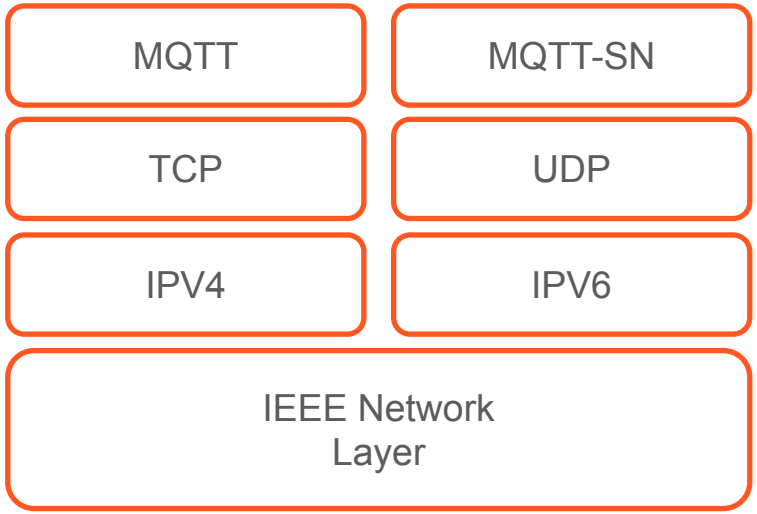
Constrained IoT Devices (low power)



MQTT IoT Device Connectivity

- MQTT V3+ (TCP).
- MQTT-SN (UDP).
- IoT devices using MQTT/MQTT-SN.
- Publish/Subscribe mechanism.
- Register MQTT topics for management and data ingestion.

Generic IoT devices (generally powered)

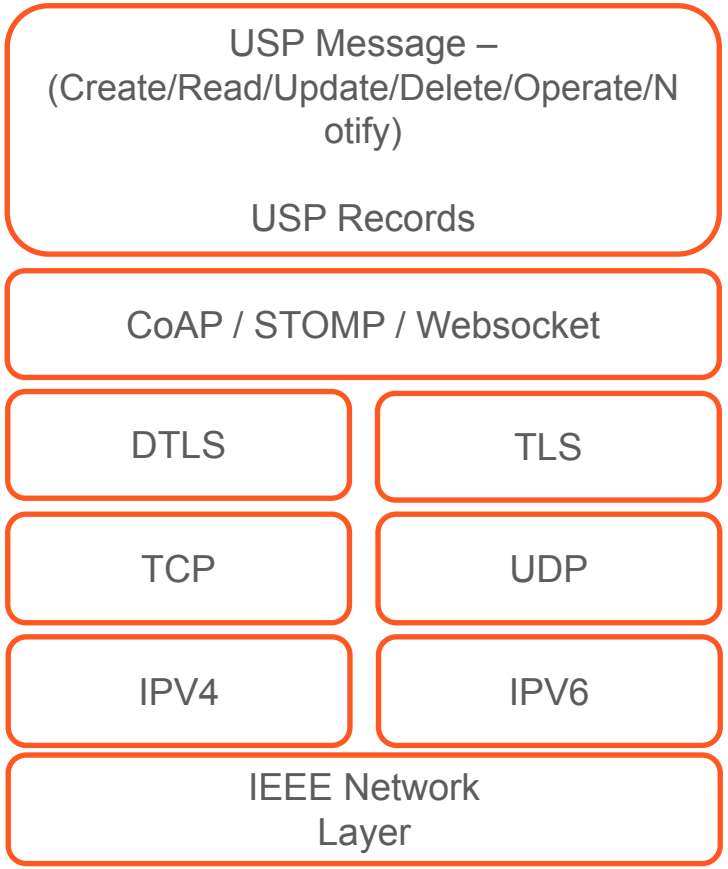


TR-069/TR-369 USP Device Connectivity

- TR-069 in older broadband devices, also used in some M2M routers.
- TR-369 USP better security.
- Better privacy, role-based access.
- Robust communications.
- Container deployments.
- Asset/sensor telemetry.

Routers & Gateways

TR-369 Protocol Stack

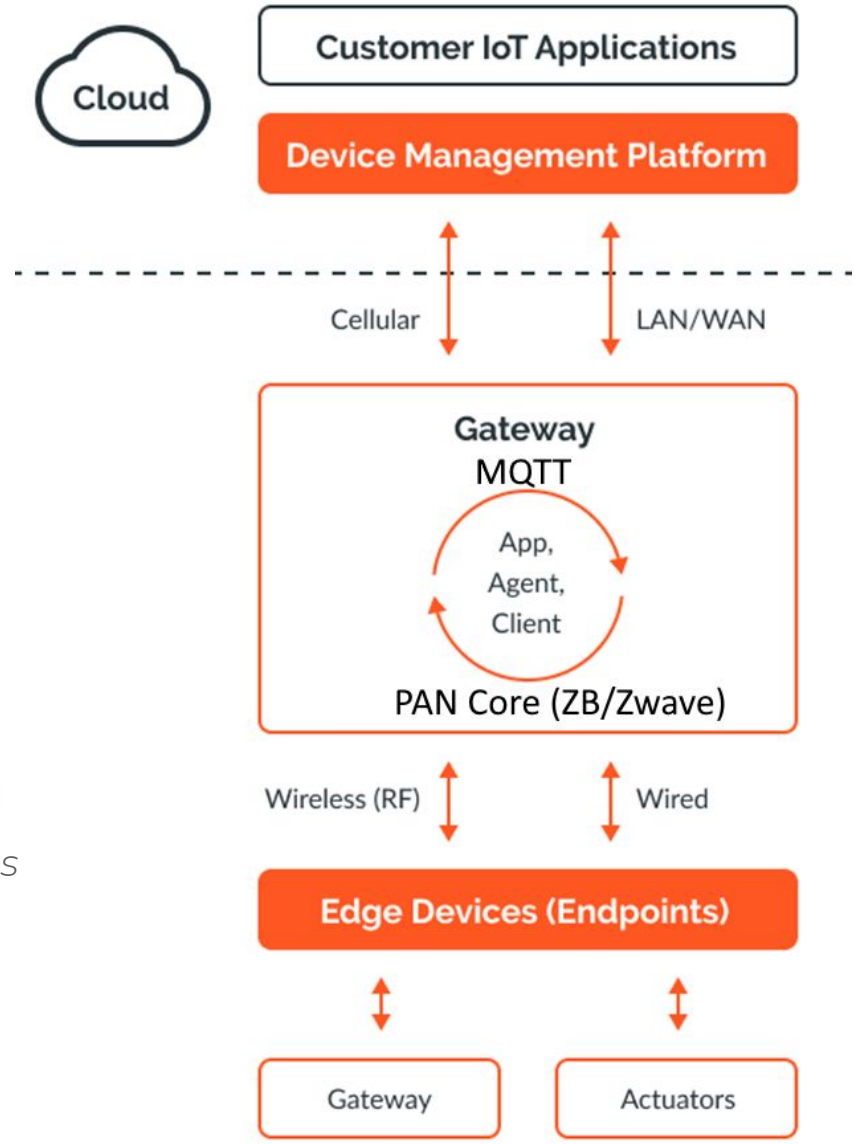


TR-069 Protocol Stack

IoT Gateway Integration

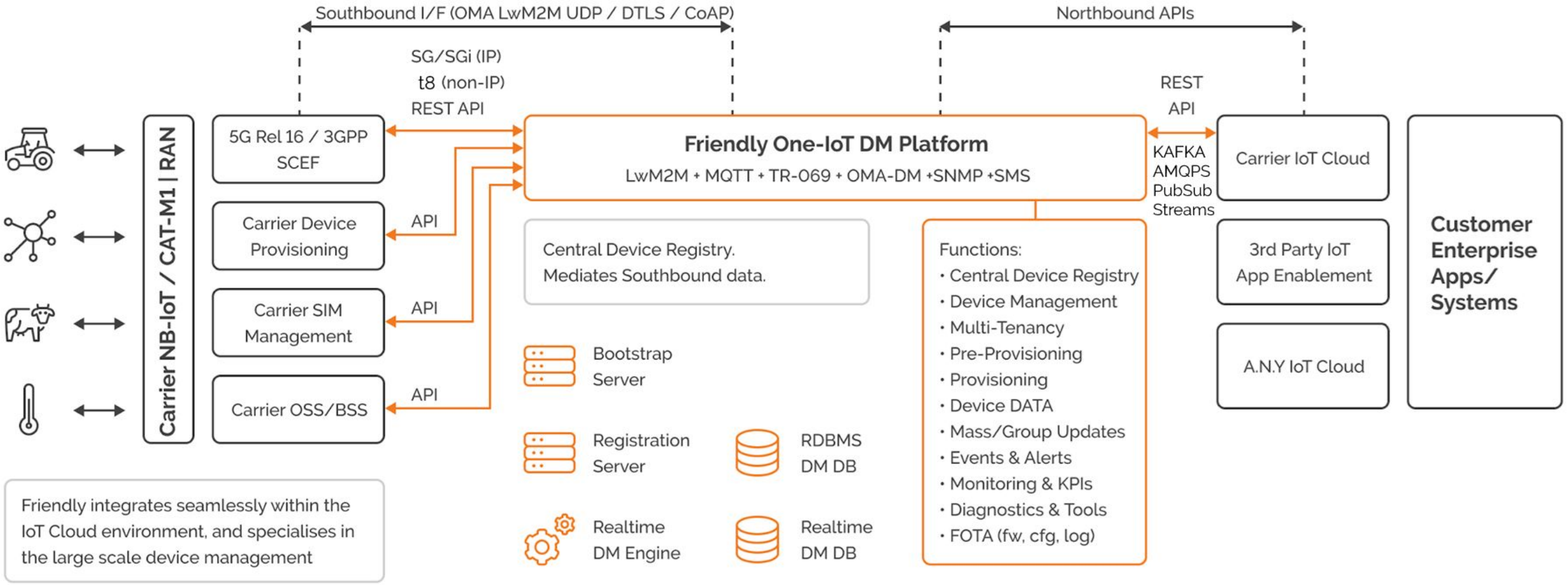
- Lack of gateway and edge device management.
- MQTT Gateway embedded client.
- Zigbee or Zwave, and others (BT/WiFi/IEEE802.15.4/6LowPAN).
- Customised client mediates the management functions to the connected sensors.

PAN Wireless Gateways

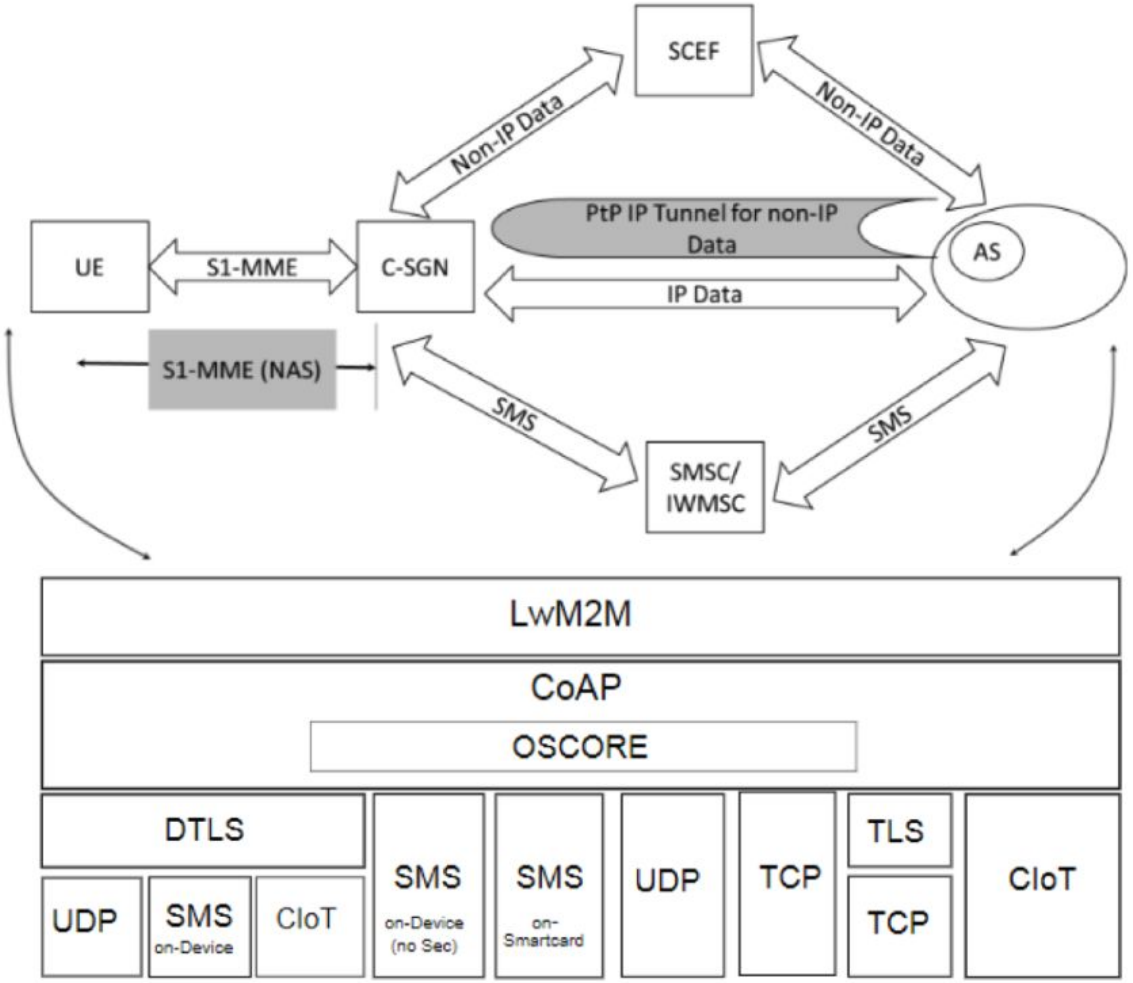


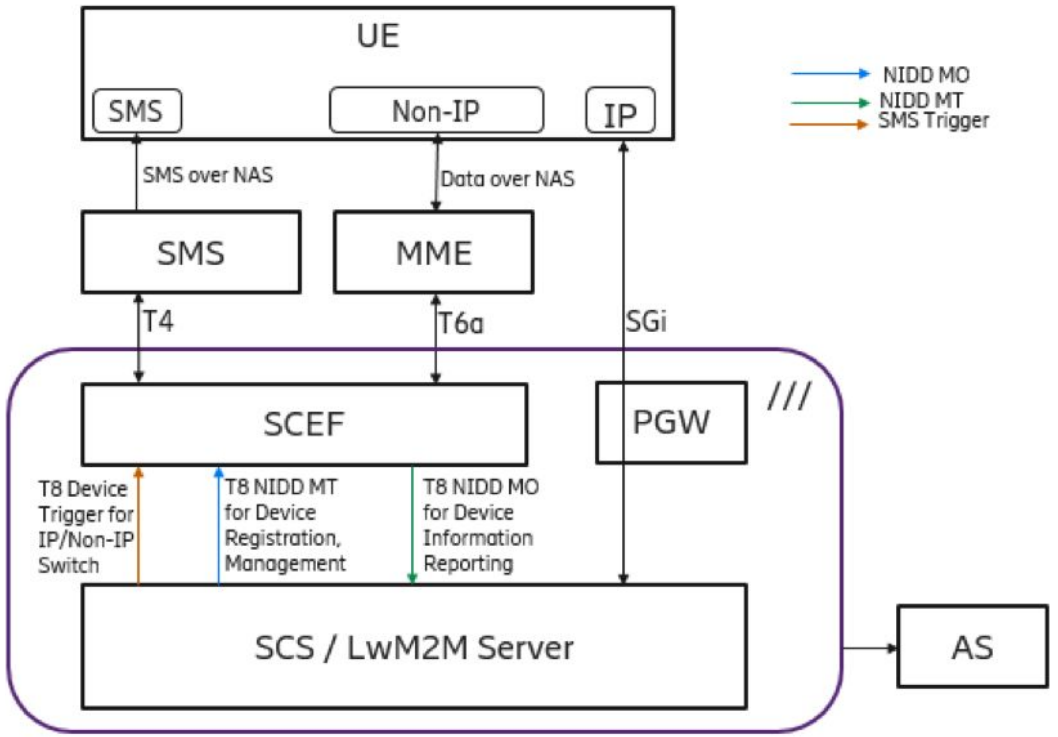
IoT Cloud – Future Proofing

Carrier Integration – Future Proofing | Device Registry



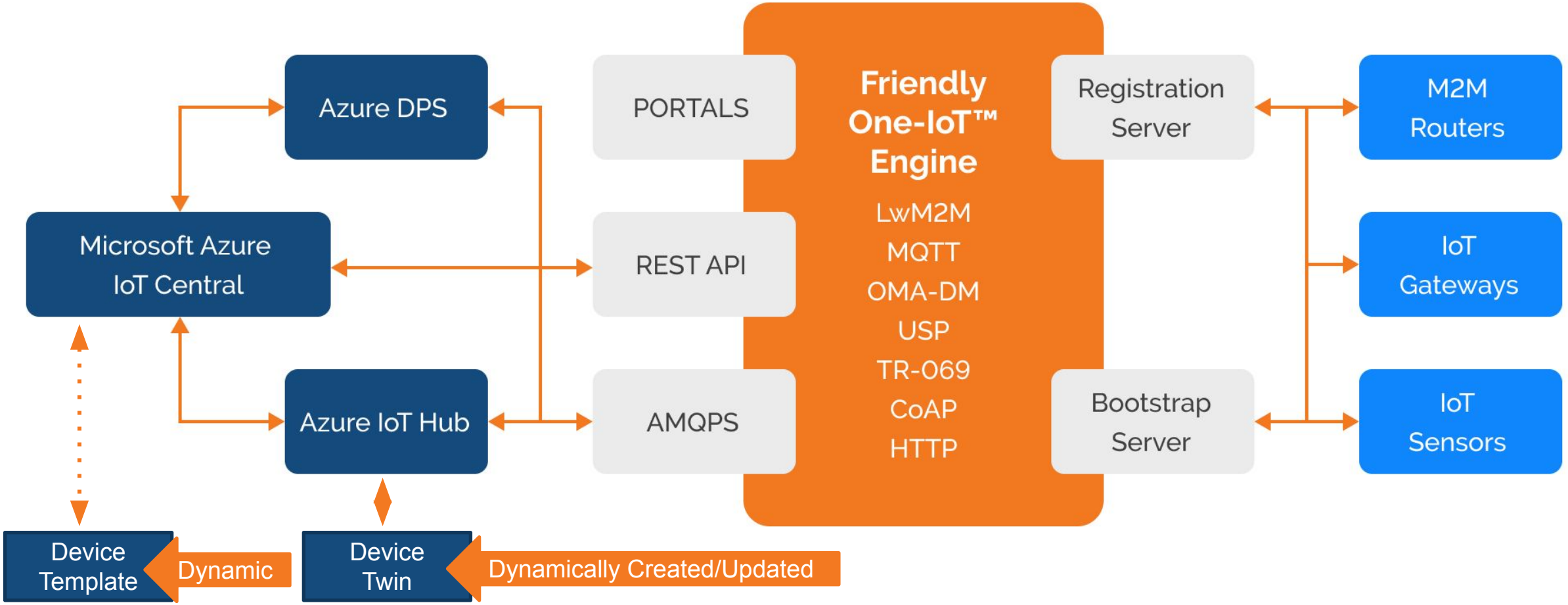
3GPP Rel 16 – SCEF & LWM2M co-existence



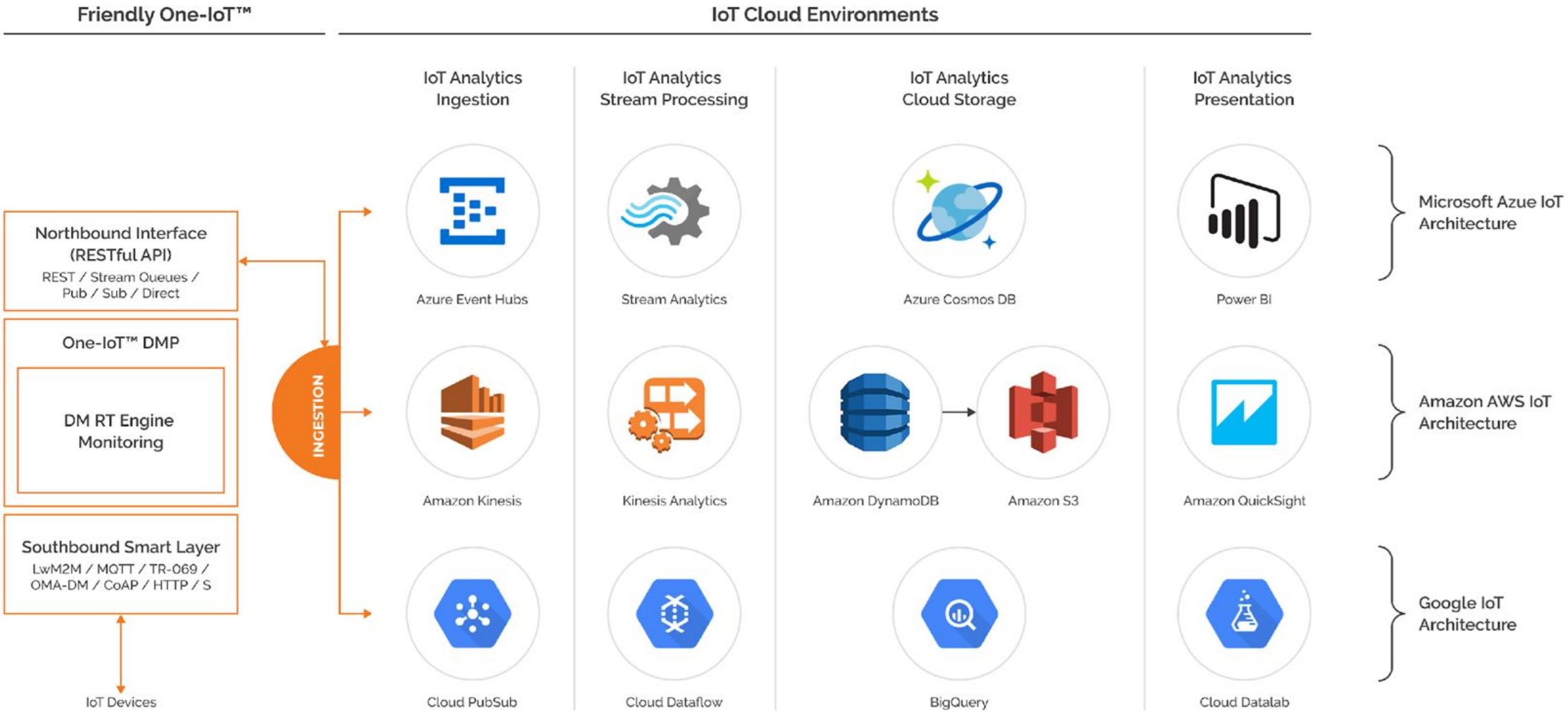


OMA Specworks - Managing Non-IP Devices in Cellular IoT Networks – [2]

Unified DM with Microsoft Azure IoT Cloud



IoT Cloud Upstream Processing



Conclusion

IoT Device Management Protocols

OMA LWM2M is the protocol of choice for IoT applications utilizing low power, low overhead, resource constrained devices, it features many benefits over other traditional protocols, such as MQTT and CoAP direct endpoints. For medium to larger footprint IoT devices, BBF's USP is arguably well placed for these more powerful IoT applications.

Some of these features include:

- A Standards based approach.
- Low Power utilization.
- Efficient over the air transmissions (management & telemetry).
- Interoperability between devices and management servers.
- Built-in Security mechanisms from transport protocols, to data protection, to Application layer security.
- Adopted by some of the largest Carriers in the world: AT&T, Verizon, Deutsche Telekom, Telefonica, Telstra, Reliance Jio and many others.

Future Proofing IoT Device Deployments

When considering to protect your IoT device fleet, for existing or future IoT device deployments, there are a few safeguards to aid your future proofing of your assets in the transition to 5G NR networks:

- DM Standards based protocols for edge devices (LWM2M and USP).
- Open protocol adaptor support to include integrating custom protocols.
- 5G NR spectrum support for LTE based LPWAN devices.
- SCEF integration for Non-IP devices (NIDD).
- Upstream IoT Cloud support using standard streams or APIs.
- Highly scalable and highly reliable Device Management Application Server, supporting IP & non-IP devices.

References

References

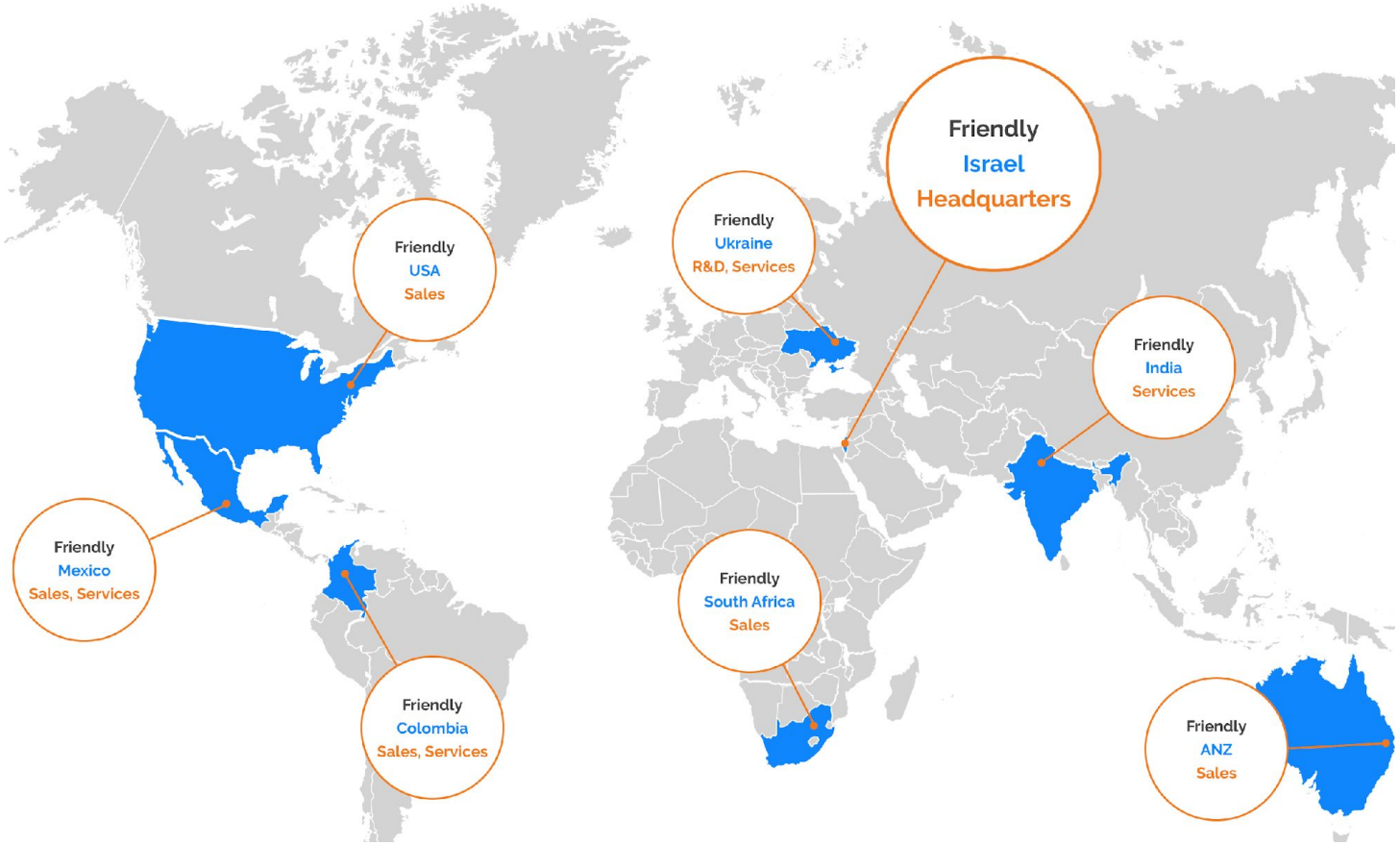
- [1] GMSA : Mobile IoT in the 5G Future - https://www.ericsson.com/4a8d35/assets/local/reports-papers/5g/doc/gsma-5g-mobile-iot.pdf
- [2] ubidots : NB-IoT vs LTE-M: Here's What The Cellular IoT Buzz Is All About - https://ubidots.com/blog/nb-iot-vs-lte-m/
- [3] – OMA Specworks : Lightweight M2M 1.1: Managing Non-IP Devices in Cellular IoT Networks - https://omaspecworks.org/managing_non-ip_devices_in_cellular_iot_networks/

- https://www.youtube.com/user/TR069FriendlyTech

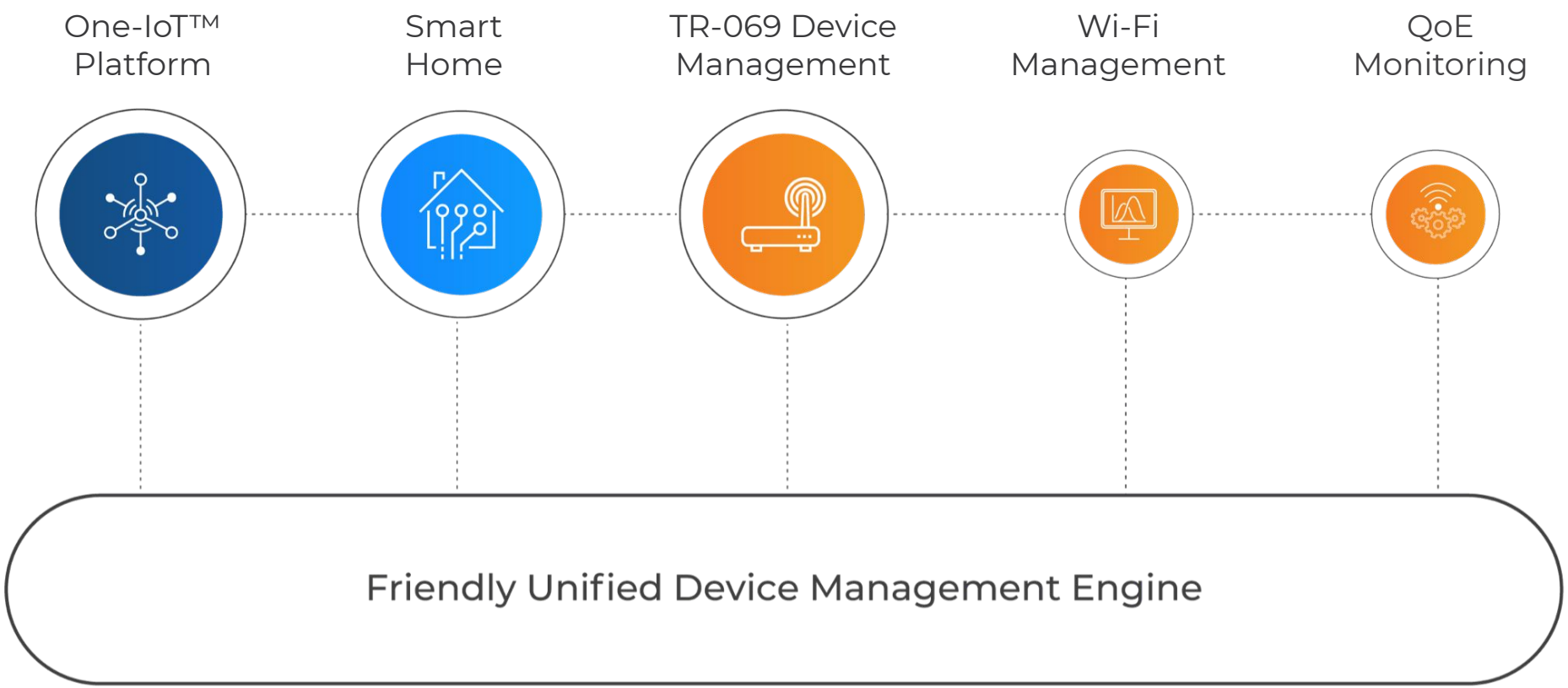
About Friendly Technologies

Friendly Technologies at a Glance

- Software company founded in 1997
- Device Management since 2006
- 200+ customers worldwide
- Active Member of Broadband Forum & Open Mobile Alliance
- The most installed Unified Device Management solution in the world



Unified Line of Products



- TR-069 client
- TR-369/USP client
- Smart Home client
- OMA-DM client
- LwM2M client

Select Customers

Success Stories

Reliance Jio (India)

The largest private company in India. Friendly was selected after in-depth market study and deployed a platform to manage **50M LTE & FTTH devices (TR-069).** Friendly was selected by Jio for **IoT Device Management.**

T-com (Romania)

T-Com Romania, a part of Deutsche Telekom group, selected Friendly's Device management for xDSL, FTTH. The solution includes **IPTV QoE** monitoring and STB management.

Beeline (Russia)

Russia's telco giant has selected Friendly's full device management solution. The DM solution was deployed in a very short time. Friendly successfully implemented an effective solution for device management over **crossed networks.**

Airtel (India)

Bharti Airtel India spent a considerable effort to evaluate and select vendors for a DM platform, managing many millions of LTE & broadband devices.
Wi-Fi monitoring diagnostics and optimization

Landis & Gyr

The global energy and utility manufacturer chose Friendly Technologies as its partner for the management of devices in the ANZ region.
IoT platform for L&G customers.

Casa Systems

NetComm Wireless (now Casa Systems) chose Friendly One-IoT™ to deploy 50K M2M routers using LwM2M for management of Coca-Cola (USA) FreeStyle fountains over AT&T and other networks. **IoT management of vending machines.**

Thank You For Your Time!