Radiocrafts
Embedded Wireless Solutions

WP015

# Radiocrafts Industrial IP Mesh - RIIM

By Ø.Nottveit/ F.Eskelund

## Introduction

Radiocrafts has developed an IP based wireless mesh solution to enable end-to-end IP communication between IoT devices and the Cloud. We call this solution RIIM, Radiocrafts Industrial IP Mesh. The use of end-to-end IP is a trend in order to reuse the networks, protocols and solutions from the normal internet in the IoT business. The benefits are that an IP- mesh solution removes the need for complex gateway solutions and allows all end points to be accessed directly from the Cloud without a proprietary addressing solution.

This document discusses the background for why these products were developed and what the benefits are to the industry that makes IP mesh a commercially attractive solution.

## Legacy M2M thinking

Machine-to-Machine (M2M has traditionally been made in vertical silos, each making their own propriety solution on data modelling, applications and protocols. Internet has for the latest years often been used as a tunnel to transport data to hook it to a cloud solution.

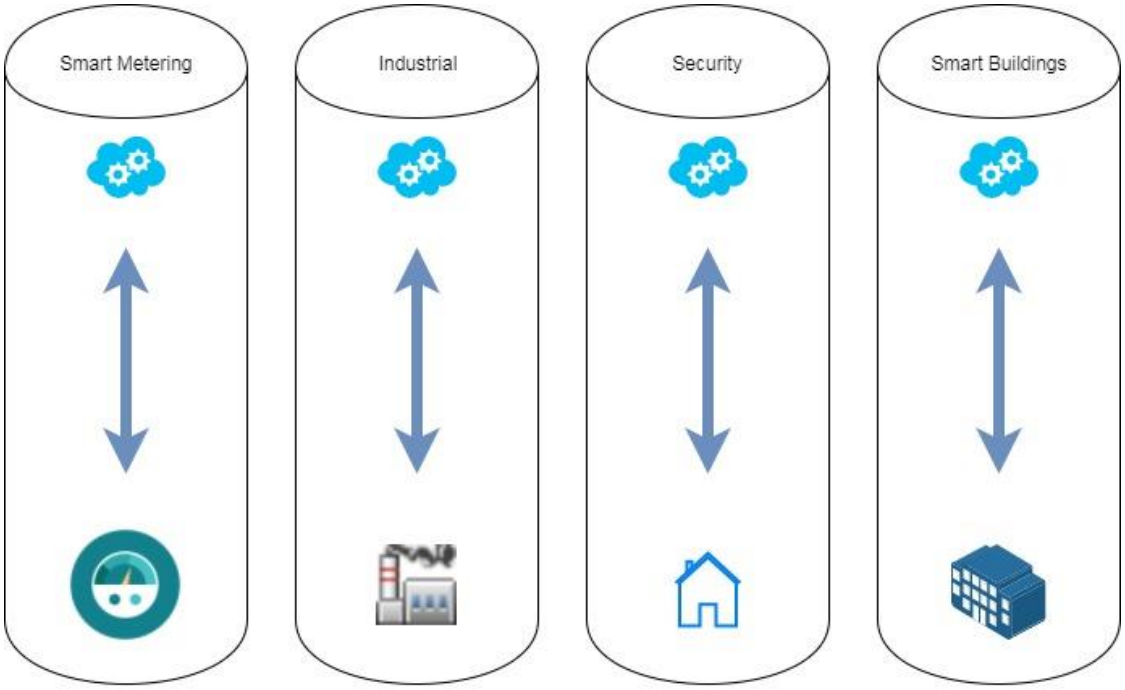
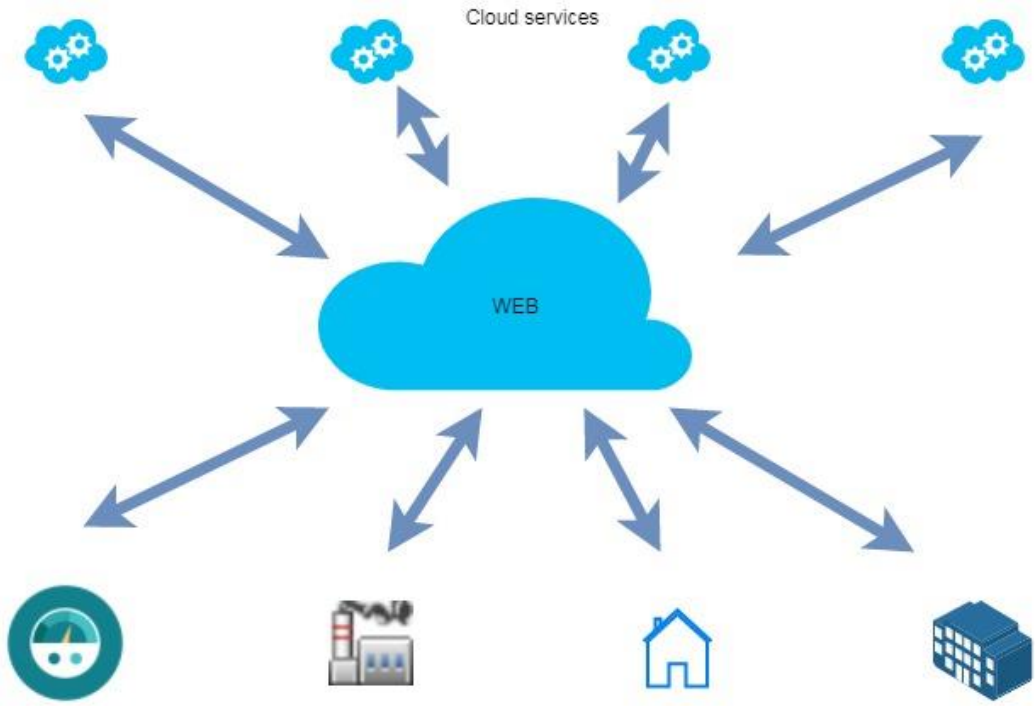



*Figure 1. M2M proprietary silos*

The challenge is that each silo contains proprietary protocols, network layers, security measures etc. This limit interoperability, portability, and maintainability and thus it limits growth.

## One uniform IoT network




IoT has become a huge and diverse business. Most data communication to a cloud server or between most IoT devices today are IP based. This give a uniform communication method between cloud service and also between a service and an IoT device.

This means the methods of communication are the same if a service gets data from a different service or from a physical device.

Device discovery, service discovery, device management, device security handling etc. will then be the same regardless of physical medium. A cloud-service might not know if device is connected via wireless or Ethernet. It only knows an IP address and a port to connect to and can therefore use standard ways of query the device on this address.

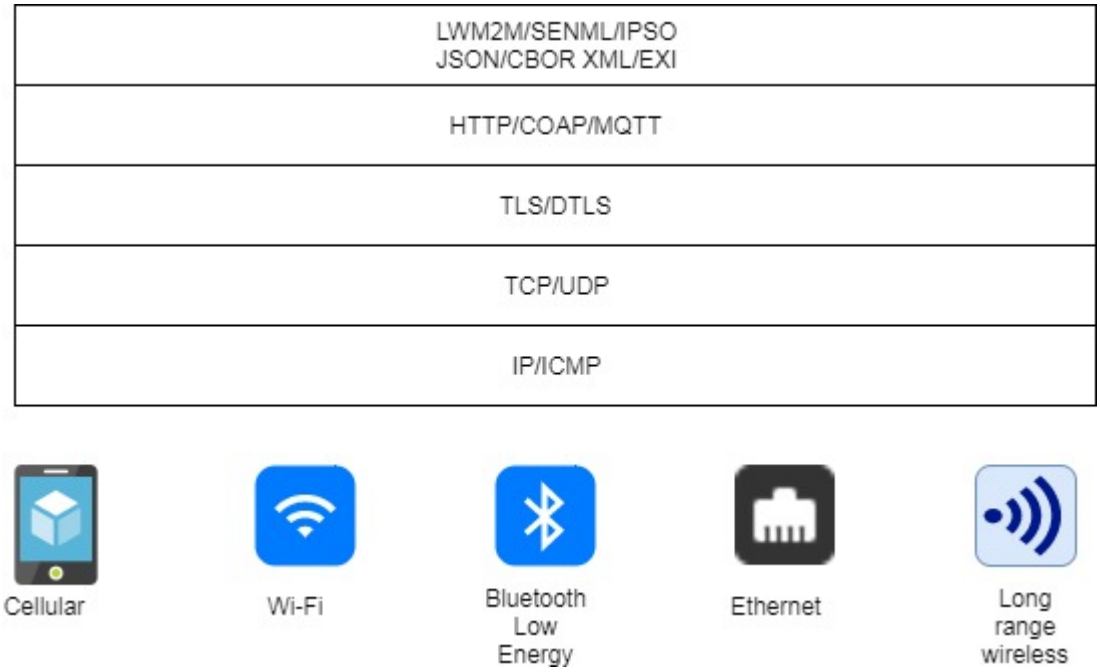



*Figure 2. Different mediums- same network protocol and methods.*

If all different sources of data used their own proprietary method for distributing and formatting data, then each service provider must have knowledge of the proprietary methods and protocols and adapt to each of them. Such solutions would not be scalable for the large and diverse IoT world.

Due to limited battery power and data rate, wireless long-range communication has normally not been IP based, but rather proprietary vertical solutions. There are two fundamentally different approaches to adapting a wireless sensor network to IP.

- By adapting IP to low power low data rate devices.
- By Proxy/Gateway

IETF and other organizations have made a tremendous effort into adapting and simplifying IP so that it suits low power, low data rate and lossy networks. Below are some standards and protocol developed for this purpose.

- 6LOWPAN
- RPL
- COAP
- CBOR
- SENML

By combining these with the well-known technologies like UDP/TCP TLS/DTLS etc. there is a complete suite of solutions available and ready to be used.

### COAP application protocol

The internet is widespread not only based on TCP/IP protocols, but also on the application protocols like http. Http was made for PC's and when evaluating HTTP for constrained devices with low bandwidth and limited processing power it is not optimal. Due to this the IETF initiate the reinvention of HTTP for such low power and constrained device. What they came up with was CoAP, HTTP's little brother that has less overhead, requires less processing than HTTP.

CoAP it standardized in many other system standards like home automation standard Thread and in the cellular industry standard LWM2M from OMA. Together with MQTT CoAP is the prominent and widespread IOT application protocol in the market today.

The difference vs MQTT is among others that MQTT is based on TCP, while CoAP is based on UDP. This makes COAP less overhead when transmitting small amounts of data.

Even though RIIM is design to use end to end IP packets, there are also possible to do application gateways somewhere on the connection and this is shown in Figure 3. The concept is basically that the transport and application layer can be converted from UDP/DTLS/COAP to TCP/TLS/MQTT (HTTP). Such a solution is more complex and challenging to setup, but it gives the advantage that the two protocol suites can be optimize for different network properties. A protocol gateway can be implemented very easily on any standard linux computer using open source conversion tools.

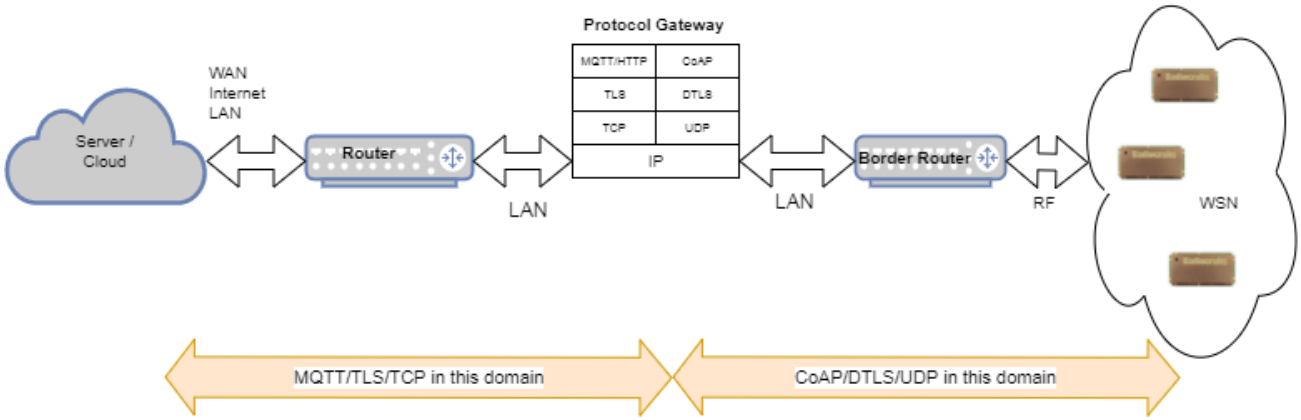



*Figure 3 - Protocol gateway concept*

### Total cost of ownership/Future proof

Selecting a wireless technology for a given solution today can be very confusing, as technology development is rapid and the different technologies are hyped up. In order to make a system with low TCO (total cost of ownership) the key is to avoid a system with risks of being obsolete and or redesigned in short timeframe.

- Avoid relying on external operator that have unproven business ideas.
- Use the best wireless chips/stack/module available now, but avoid adjusting the entire infrastructure on chosen low level technology.
- Make room for adding tomorrow's new and improved technology seamless into your existing solution.

All the advices above will guide in the direction of an IP based wireless solution that can combine long range wireless sensor network (RIIM) with other technologies like Ethernet based device, NB-IoT, BLE etc.

### Scalability

One of the principle challenges in IoT is the huge number of devices and the addressability of them. This is part of the reason that the number of available IPv4 addresses for new products are going toward zero and that the IETF introduced IPv6. IPv6 increases the number of available addresses significantly, which will ensure that every IoT device can get its own IP address which can be valid globally.

### One unified network or dual network

There is no question that IoT communication will rely heavily on IP protocols in the future and IP must be used at some level. The options are to use an end-to-end IP solution or to use different communication on the last mile to the end devices and proxy these technologies to IP network in a complex gateway.

Historically this proxy method has been done with the reason that

- IP stack is too big and require too much processing power for end nodes
- IP communication create too much overhead.
- IP communication does not create power efficient nodes.

There have been leaps in progress for IP-based end nodes over the last years.
Where MCU previously often have limited flash to maybe 32 kB or 64 kB, today many standard MCU are set up with 256 kB-1MB flash. The processing power and efficiency of MCUs are also constantly increasing at an impressive rate.

The IP stack has also been miniaturized and a miniature IP stack now can take as little as 50 kB of space. Therefore, the first argument vs. IP is no longer valid.

There has also been done a huge effort in developing the IP standards to minimize overhead and thus power usage. This is now available in standards like 6LoWPAN, CoAP and CBOR.
These standards significantly reduce the overhead with IP and the overhead can be in order of tens of bytes.

Compared to optimized, proprietary solutions there is still a small increase in overhead with IP, but in most cases the IP overhead is not limiting and solutions with 10 years battery lifetime can be realized.

### Security (DTLS/TLS)

When using IP based networks all security mechanism can be utilized end to end. That means protocols like DTLS/TLS can be used between end nodes and endpoint in the cloud service. This way the gateway does not know the encryption keys used, and any hacking of the gateway will not threaten the confidentially of data end to end.

This present a huge advantage toward existing solution with proxy gateway. There the gateway itself have the data unsecure and the gateway itself becomes a security vulnerability.

TLS/DTLS is the state of the art security mechanism used in the internet and gives future proof system and known protocols for the cloud developer compared to using proprietary security protocols that might be outdated, buggy and unknown to network operator.

### Coverage/Mesh

LPWAN is commonly used term for long range IoT networks. There are several ways to get larger coverage.

- Use higher output power (Normally limited by regulation)
- Better sensitivity. (No leaps in technology, so only way to achieve this is by reducing data rate.
- Multi-hop/mesh solution. (Requires router)

The basic advantage of mesh is greater coverage. Any router device can forward data from one node to the next and communication between devices normally out of radio range is possible. By using a mesh, the end devices/sleeping node can continue to send short/energy efficient packets and thus have long battery lifetime, while still be spread over a wider area.

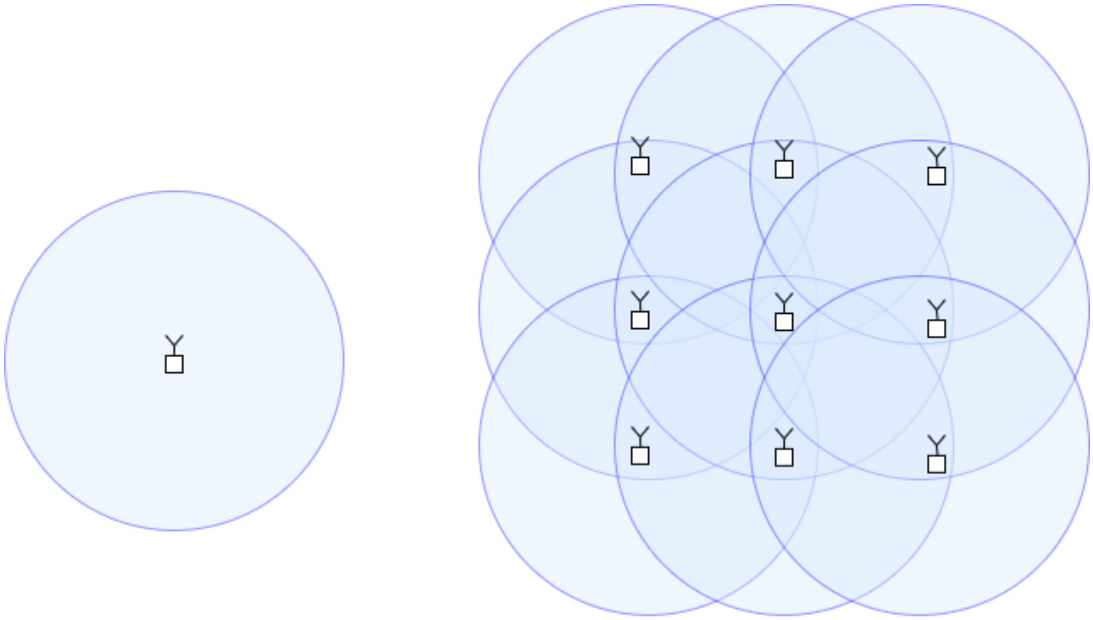


*Figure 4. Coverage of one device (left) and coverage of a mesh with 9 devices (right)*

Due to the higher data rate all link packets can be acknowledged and thus give reliability. Due to the mesh concept there are no single point of failure. If one device fails, the network will self-heal and new data paths will be made to go around the broken device.

The mesh topology used in RIIM enable completely self-configuring and self-healing networks. This means that no network management is needed. An intelligence is included in each node to find the optimized route to the border router to ensure the most reliable connection.

The max number of nodes in the mesh is not a fixed number. It will be affected by the topology, data packet sizes, data traffic, security setting etc. RIIM utilize source routing down into the network. This limit the memory requirement on each routing mesh device, and require more memory on the border router. The border router in RIIM contains >4 times the amount of RAM compared to the child nodes and thus allow several hundred nodes given that the data traffic to each is limited.
But all large network should be verified with the actual data traffic pattern and topology intended.

### Reliable, low power and low latency through 6TiSCH

As part of the IP development for low power low data rate network, 6TiSCH has also been developed. It defines how IPv6 can be used together with TSCH (Time Slotted Frequency Hopping). TSCH was introduced in IEEE 802.15.4:2012 and is a combination of Time division multiple access and Frequency-division multiple access. This means that transmissions are done at several frequencies and at different time slots in a synchronized schedule.

TSCH give very high reliability, low predictable latency and low power. The use of multiple frequencies gives robustness against jamming, noise, collisions and multipath problems. As the time slots are well defined, the latency of a packet from one node to another is deterministic. The use of timeslots also gives the nodes a defined time to go to sleep and thereby conserve power in an efficient way.

### OTA Firmware Update

A very important feature for future proofing the network is the Over the Air (OTA) capabilities. The pace of innovation and change in the IoT business is rapid and imagining a firmware being fixed without modifications for 10 years seem unlikely. Due to this capability to upgrade the firmware from a central point is a key capability.

For OTA the RIIM has implemented an OAD function based on CoAP packets Over UPD. This is the same concept chosen for OAD in LWM2M-standard from the Open Mobile Alliance.

The new firmware image received via RF is stored in a flash memory and is normally encrypted. The image is decrypted, verified and authenticated before loaded into active memory in order to protect against malware or hacking.

### ICI (i:zi), Application development in no time.

One of the unique features of the RIIM suite is the ease of development. As chips, stacks and solutions are becoming more and more feature rich, the complexity also increases. 10 years ago a typical sensor application was written as bare metal code based on super loop/while(1) loop in 8-16 kB of code.

Today's solutions are often based on an OS, a complex stack and high-level security giving a total of 100kB+. When solutions are becoming more complex, they easily require longer development cycles with higher risk.

To combat this, Radiocrafts introduces the ICI (i:zi) concept for intelligent C-programmable sensor and actuator interfaces and control at the end nodes. The core of ICI (i:zi) is to abstract all the complexity of the solution and give the user an easy and intuitive API to write his code.

Example: The user has his specific requirement like:

- When I press a button device shall try to join
- When joining successful blink green led.
- Read an I2C sensor every 15 seconds.
    - If above a certain level send alarm via RF
- Send last read sensor value every 5 minutes (even without alarm)
- Allow the Cloud application to send message in changing the *sensor_ interval* and *threshold*

The ICI (i:zi) concept allows the user to write his six different event handlers from above example without any knowledge of the architecture of the hardware and avoid spending time interfacing to the wireless stack, threads in the RTOS system and inter-thread communication and other complex issues.

### Border router (Gateway) solution

In normal legacy M2M, the gateway needs to implement the IoT agent. This means that the gateway is the end point for the internet connection. Basically, the gateway becomes a broker between the IP based traffic on one side and the wireless network on the other. Any incoming packet from one network must be decoded and analyzed and the mapping function to what packet to send out on the other network must be done.

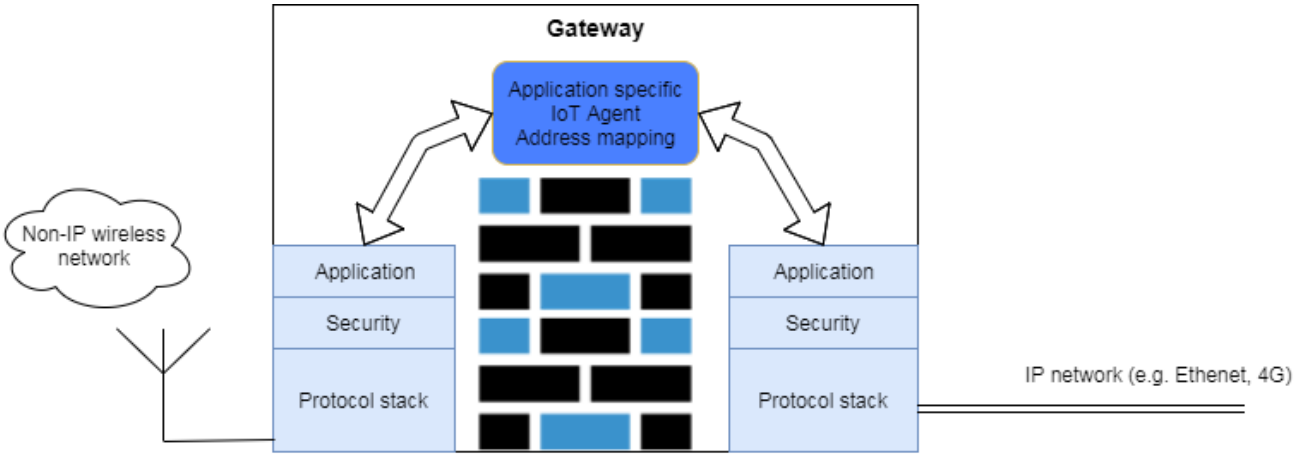



*Figure 5. The gateway concept*

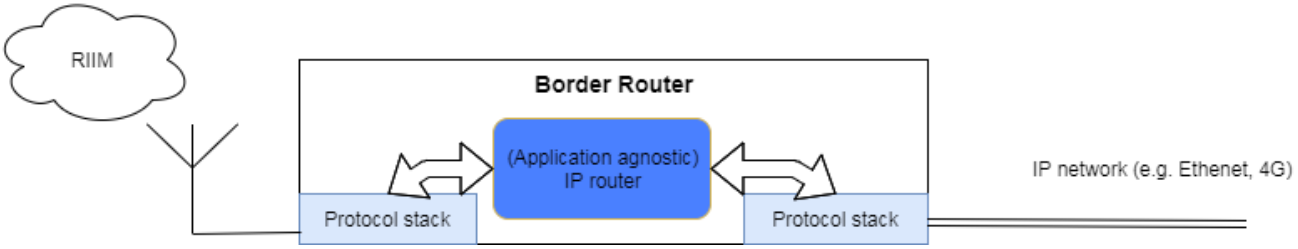



*Figure 6. The border router concept*

The IoT agent in the gateway becomes quite complex and need to include address mapping, mapping packet types in one protocol to packet type on the other protocol. It must map the application packet and it must map the IP addresses to a local address.

With IP mesh, there is no need for a Gateway. The end point contains the IoT agent and the work of the border router is simply to route the IP packets from wireless network to the WAN. Due to this the box connecting a wireless IP mesh network to the wired internet are normally referred to as border router or edge router.
All addressing, encryption and application messages goes end-to-end, and this enhance security and reduce complexity.

Since the border router is a generic device that can be reused in many different applications, Radiocrafts have developed our own border router device that can be utilized directly as a product without further development cost.


*Figure 7. Radiocrafts RIIM Border Router*

## Summary

Through this document the arguments for using end to end IP has been advocated and the historical reasons why not to use end-to-end IP has been analyzed.

There are several reasons why to use IP:

- Scalability
- Uniform network
- Future proof
- Reliability
- Well tested technology
- Based on global agreed-upon standards
- Removes proxy and translation complexity
- Removes need for complex hardware (Gateway vs. Border Router)
- Uses off the shelf HW

## Document Revision History

| Document Revision | Changes |
|---|---|
| 1.0 | First release |
| 1.1 | Added info on border router and more detailed on CoAP and protocol gateways |

## Disclaimer

Radiocrafts AS believes the information contained herein is correct and accurate at the time of this printing. However, Radiocrafts AS reserves the right to make changes to this product without notice. Radiocrafts AS does not assume any responsibility for the use of the described product; neither does it convey any license under its patent rights, or the rights of others. The latest updates are available at the Radiocrafts website or by contacting Radiocrafts directly.

As far as possible, major changes of product specifications and functionality, will be stated in product specific Errata Notes published at the Radiocrafts website. Customers are encouraged to check regularly for the most recent updates on products and support tools.

## Trademarks

All other trademarks, registered trademarks and product names are the sole property of their respective owners.

## Life Support Policy

This Radiocrafts product is not designed for use in life support appliances, devices, or other systems where malfunction can reasonably be expected to result in significant personal injury to the user, or as a critical component in any life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness. Radiocrafts AS customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Radiocrafts AS for any damages resulting from any improper use or sale.

## Radiocrafts Support:

Knowledge base: https://radiocrafts.com/knowledge-base/
Application notes library: https://radiocrafts.com/resources/application-notes/
Whitepapers: https://radiocrafts.com/resources/articles-white-papers/
Technology overview: https://radiocrafts.com/technologies/
RF Wireless Expert Training: https://radiocrafts.com/resources/rf-wireless-expert-training/

## Contact Radiocrafts

Sales requests: https://radiocrafts.com/contact/