Radiocrafts
Embedded Wireless Solutions

Fast to Market. Proven Quality.

AN058: Nodes Commissioning in RIIM™

By: Ørjan Nottveit
Omar Khalil
Update 2024-06-20

Nodes Commissioning in RIIM™

by Omar Khalil and Ørjan Nottveit

Background

When thinking about networks, we often limit our thinking to the operational part of the network life, where the network is doing its intended task, like collecting sensor readings for example. However, this is not the complete picture. In real life scenarios, there are a number of questions which still need to be answered:
For example:

- *How do nodes connect to the network at the beginning of a network's life?*
- *How do nodes make sure they connect to the correct and intended network?*
- *How can the user make sure no intruder nodes can join the network?*
- *How are network-formation handled in a secure manner?*

Furthermore, there is still the topic of node discovery. For example, consider a simple 5 temperature sensors network, deployed in a house. At the very first temperature reading being reported, how will the root node know which of these 5 reading is coming from the kitchen, which is coming from the garage, and so on. The same kind of challenge applies for smart irrigation networks for instance. If the root node gets a report that a certain area is dry, it must ensure it initiates irrigation in that particular area, and not another.

All the above-mentioned challenges are the reason why discussing nodes commissioning is very important. Correct and secure nodes commissioning enables a seamless start to the network.

This document aims to give the user a basic overview of commissioning processes in general, such as network formation, service discovery, and device discovery. Furthermore, the document also aims to shed more light on how RIIM™ handles different aspects of commissioning and what processes Radiocrafts suggests for different commissioning aspect.

Figure 1. The three steps of commissioning

What is Nodes Commissioning

Nodes' commissioning is a broad term that encompasses a variety of network operations. Simply, it can be defined as all network operations which take place before the real operation of the network starts. It can also be defined from a device's point of view, as the process of giving that device the necessary information to join a network successfully and securely. From a network's point of view, a possible definition for commissioning could

mean the process by which the network's central node (be it a Border Router as in a RIIM™ network or the cloud) identifies a new node and maps its device ID to its real location or function.

This can mean that the commissioning stage includes, network formation, device discovery, and service discovery. It is important to note that nodes commissioning is not necessarily a process that happens only at the beginning of the network life, it can also refer to the process of adding a new node to an already existing network.

Network Formation

Joining the Correct Network

As a first step to a successful network setup, child nodes must be able to join the correct network. It is sometimes easy to forget the not all users plan to setup their networks in a secluded area, and that there is always the possibility that the network's location will be close to another already-operational RIIM™ network. This might cause nodes to join a wrong network at startup.

In RIIM™, a network can be identified in two ways, using the PAN ID and the Network Shared Key. To ensure that nodes join the intended network, all nodes in this network should share a "unique" PAN-ID and network key. So, the commissioning challenge is to get these credentials into each node. These two parameters can be entered by the user into the module through his ICI application (the C-based interface where the user controls the high-level aspects of the module's functions).

As discussed earlier, entering such parameters manually to each node and even having them hardcoded at the manufacturing phase can pose a logistical and tracking challenge. Therefore, it is more optimal to use commissioning methods which are logistically feasible, and at the same time ensure a correct and efficient commission process.

There are 3 different ways to enable nodes to join the correct network:

- *Pre-commissioning in factory*
- *Setup at installation location with tool (dip switches, NFC, BLE)*
- *Setup with Joining PAN-ID*
    - *Either the actual BR goes into commissioning mode*
    - *Or a separate tool in terms of a dedicated commissioning BR*
    - *Setup to join any PAN-ID*

Pre-commissioning in the factory

The simplest way to commission a network with correct PAN-ID and network key is to do this at the factory. But this requires that the business is project-oriented such that it is known on the factory floor which devices shall be used in which project/installation. In many cases this is not known and then it becomes logistically challenging to commission devices already on the factory floor.

Setup at installation location with tool (dip switches, NFC, BLE)

A second option is to handle commissioning at the installation site by the installer. A commonly used option would be to commission nodes in the field by using a short-range RF technology such as Bluetooth, NFC, or even by setting certain parameters of the node by using dip switches. This way, all nodes can be shipped from the manufacturer carrying the same settings, which reduces tracking and logistical challenges. Then the nodes would be placed in their positions in the field as the user intends,

Afterwards, the user would program his Near Field Communications (NFC) device for example, to communicate with the NFC chip in the final product. The NFC programing device would tell the node which PAN ID and Network Shared key to use, according to the Border Router being used for this network.

This solution might add some extra costs to the total network cost, but it obviously takes the least time and effort. It is a commonly used methods for business where professional installers are used.

Setup with Joining PAN-ID

Some use cases require that there is no action on-site by an installer as this is a source for mistakes. They then often require a "touch-free" commissioning. This can be accomplished by using dedicated credentials for a commissioning network

- ***Initial Network Setup- Scenario A***

Let's assume the user is setting up their network for the first time. A possible solution to commission the nodes and have them join the correct network is shown in figure 2 below.

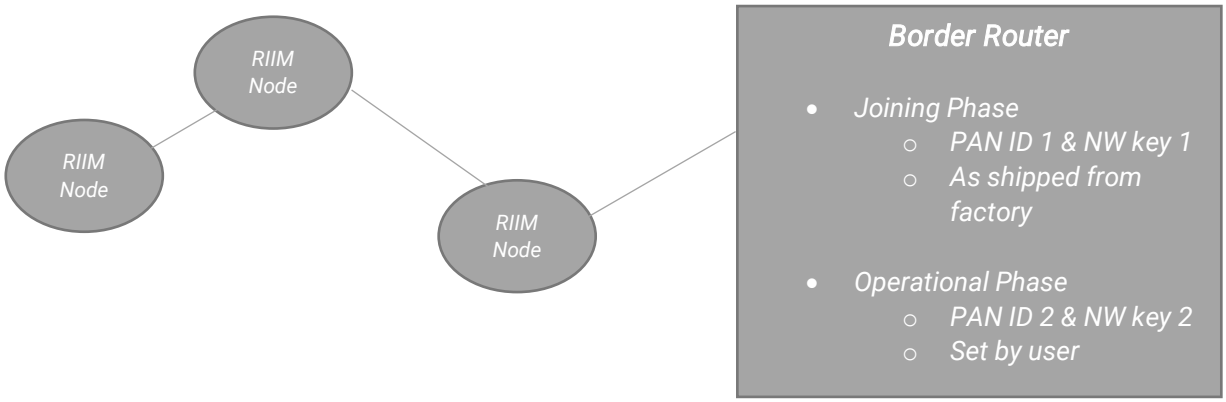


Figure 2. Scenario A Commissioning

In this scenario, nodes are shipped out from the factory with a default PAN ID and Network Shared Key, corresponding to keys 1 in figure 2 above. The Border Router can be programmed to switch to keys 1 with a button press, this will allow all nodes to connect to the Border Router. Thereafter, after the network formation phase is complete, a C function in the Border Router code can be called to broadcast a new set of PAN ID and NW key, corresponding to keys 2, to the nodes, followed by a reset command.

This way, the nodes would restart and join the Border Router on its new network credentials. This would prevent any extra unwanted node to join, as the keys set 2 set are secret and no other nodes are expected to be aware of it.

- ***Adding and extra node based on scenario A***

Using the same logic of scenario A, adding a new node can be done by going through the same procedure. The user receives a new node from their factory. That new node is expected to have the keys 1 set. Upon a button push on the Border Router, it would switch to keys 1 and allow that new node to join. Then, as explained above, the Border Router would give the new node the keys set 2 and order it to restart.

The only drawback to this procedure is that the nodes which have already joined in scenario A, will be left without a network while the Border Router commissions the new node being added. This is not optimal. Therefore, let's examine scenario B.

- ***Initial Network Setup Using 2 Border Routers- Scenario B***

A possible solution for the issue mentioned above would be the use of a special Border Router, used as an extra only for commissioning purposes, let's call it Border Router C (BR_C) and let's call the original Border Router BR_P. This BR_C can be set to transmit with minimal power, to make sure no far away nodes can listen to it.

BR_C can be set to operate on the default keys which nodes are shipped with, called key set 1 in our example. When the user receives their nodes for deployment, they deploy the nodes at first very close to BR_C, to enable nodes to hear BR_C since it transmits with very low power. Nodes would then join BR_C then it would broadcast to the nodes the credentials to join BR_P and reset.

Upon the reset, nodes should start with keys set 2 and join the original Border Router BR_P for normal operation.

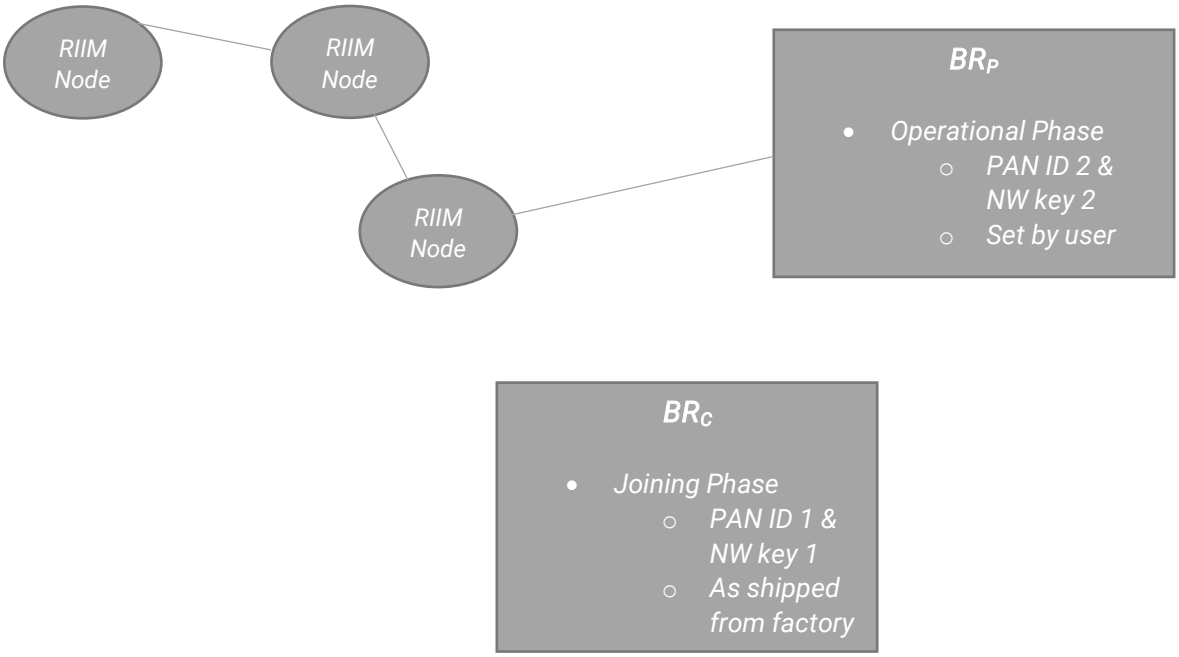


Figure 3. Scenario B Commissioning

Adding an extra node based on scenario B

Following the same logic used in scenario B, an extra node can be added, and its commissioning process can take place via BR_C. When the new node is introduced, it will search for a network with those default settings, it would find BR_C and connect to it. Then BR_C, after a certain time or after establishing the network, would order the node to change its settings to the settings of BR_P and reset. This way, upon reset, the node would join BR_P and the already established network.

Setup to join any PAN-ID

This is a method where the nodes join the first network it finds. With only one network in the area this is a very easy method. If more networks are in the same location, then some additional steps are required as described below in chapter (

Multiple Networks Collocated)

Multiple Networks Collocated

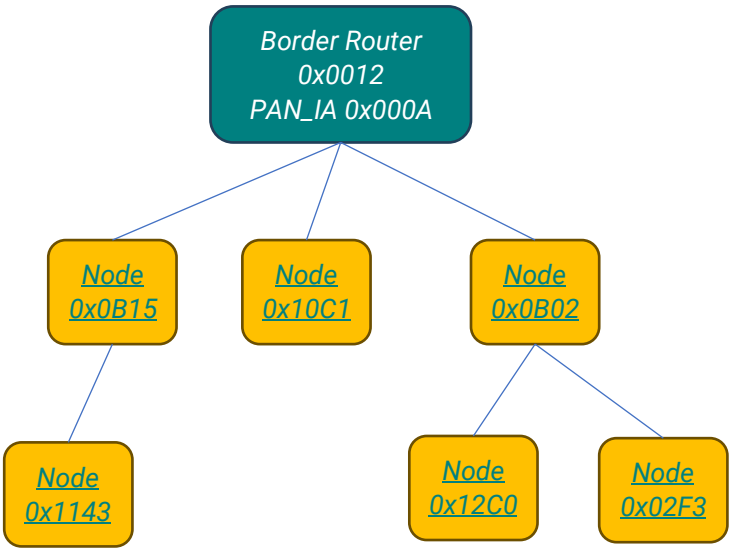
In some use cases there are multiple networks forming in the same geographical area. An example is a solar plant where each tracker is a node in a RIIM network. There can be thousands of trackers in one area, but it is not optimal to have all of them in one common network. It is better to divide the network into several sub-networks, each given by a dedicated border router and a specific PAN-ID.

As described above, one way to approach such challenging commissioning is to ***pre-commission*** *everything beforehand in the factory. This means the map of tracker and their ID + network they should be on is set at the factory. This is not a very flexible system, and it requires a lot of logistic planning.*

A more flexible way is to do this in the field. There are two alternative approaches in the field. ***Local commissioning*** *can be done e.g. by NFC and by physical accessing the plant and walking around each node can be given a specific PAN-ID via NFC based on its position and which power network its panel are connected to.*

*A third way is to do the commissioning via the radio network(****Over-the-air commissioning****). All the node setup to PAN-ID 0xFFFF, this means they will join any(the first) network/PAN-ID they find. This will naturally lead to many nodes joining "wrong" network.*

The border routers(gateways) for each network need to be started before the trackers around it are activated on radio. Addressing the border router, a central server can extract the network of trackers connected to it. And then through IP/UDP/CoAP one can readout the ID of each device.



Pseudo-code

CoAP.Get(0x0012, network)
CoAP.Response(
0x0B15-0x0012
0x1143-0x0B15
0x10C1-0x0012
0x0B02-0x0012
0x12C0-0x0B02
0x02F3-0x0B02)

CoAP.Get(0x12C0, ID)
CoAP.Response(0x0012B4230123F121)

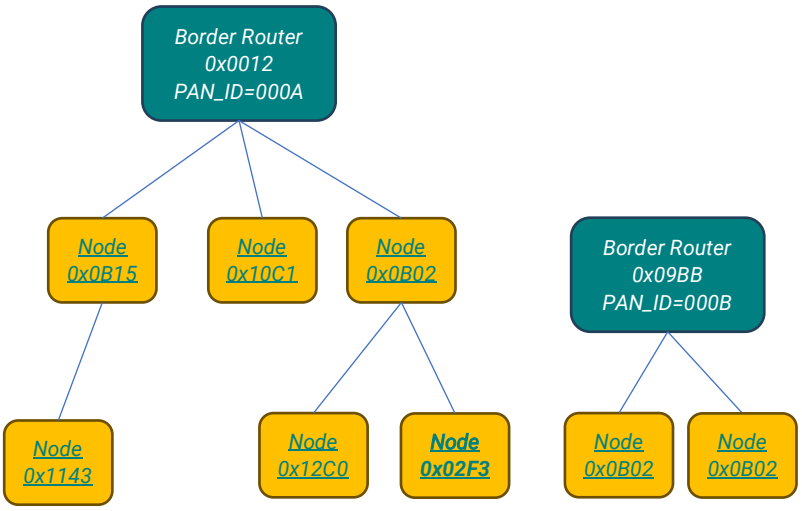
Figure 4 Device discovery in RIIM

Then the server must decide for each tracker; Is it on the optimal network and which network should it be on ideally. The criteria can vary case-by-base. Elements that can influence this commissioning algorithm includes

- *Nodes in the different networks*
  - *There should not be one huge network and one tiny.*
  - *Huge network leads to less throughput per device, longer latencies and increased risk of network congestion*
- *Number of hops from border router*
  - *Optimize for few hops*
  - *Many hops lead to more network traffic, less throughput and higher latency.*

- *Geographical position*
  - *Optimize to have trackers joining network given by the closest border router.*
  - *Close physical distance give fewer radio hops*
- *Which inverter power network a tracker is connected to*
  - *Sometimes er see that there is a logical reason for some devices to be in a common network. For solar trackers this is which power network they are connected to.*

The two first parameters the RIIM network gives out data on. The two last information elements (geo-position and power network) must be acquired with other means.



Pseudo-code

CoAP.Put(0x02F3, PAN_ID=0x000B) network)
CoAP.Response(ACK)

CoAP.Put(0x02F3, RestartRadio=True)
CoAP.Response(ACK)

Node 0x02F3 restart limiting network search to PAN_ID 0x000B

Figure 5 Original networks

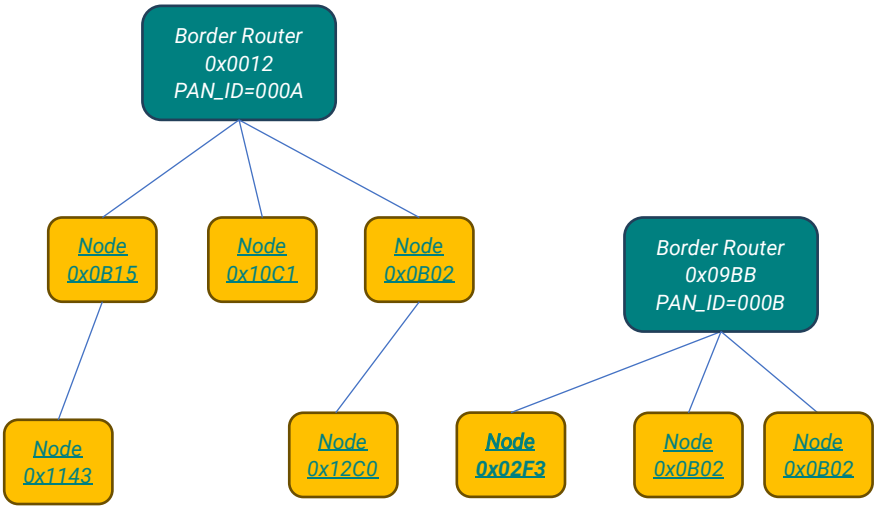


Figure 6 Network after node 0x02F3 is redirected

A couple of guidelines for over-the-air commissioning.

- *Make sure to power on border router before trackers in an area.*
- *Avoid start sending much data until all nodes are commissioned*
- *Commission gradually. That means, do not wait until e.g. 10000 tracker are installed.*

These guidelines will make the commissioning process easier as large network or congested network traffic is avoided.

Joining speed

In RIIM with TSCH (frequency hopping), the frequency hopping synchronization adds some delay to the joining process. The time to get frequency hopping synchronization depends on how often the existing network is sending announcements of the network in terms of Enhanced Beacons (EB).

The more often EBs are sent the easier the quicker joining becomes. However, sending very frequent EBs will reduce data throughput and also consume battery.

To overcome this trade-off, it is highly recommended to have different states of the system.

- *Commissioning state (e.g., 5 minutes after power up or 5 minutes after commissioning button is pressed)*
  - *Frequency EB (e.g., every 1 or 2 seconds)*
- *Operational stage(When network is stable)*
  - *Infrequency EB (e.g., every 64 or 128 second)*

These states can easily be setup with an ICI application.

Device Discovery

Consider a temperature sensor network deployed in a huge factory, and the logic is that when the temperature rises in a certain compartment in the factory, the central node signals the ventillation vents to open at that specific compartment. For this to work, the root node must collect information about the addresses of nodes and their locations. This is achieved by having a solid Device Discovery scheme.

In RIIM, all nodes are assigned IPv6 addresses when joining, in addition to a two-bytes short address. Each node signs-in with the border routers as part of joining, so the border router knows the IPv6 address of all nodes in the network. In addition each node after network joining knows the IPv6 address of the border router, but not of any other nodes. These are all shown in Figure 7.

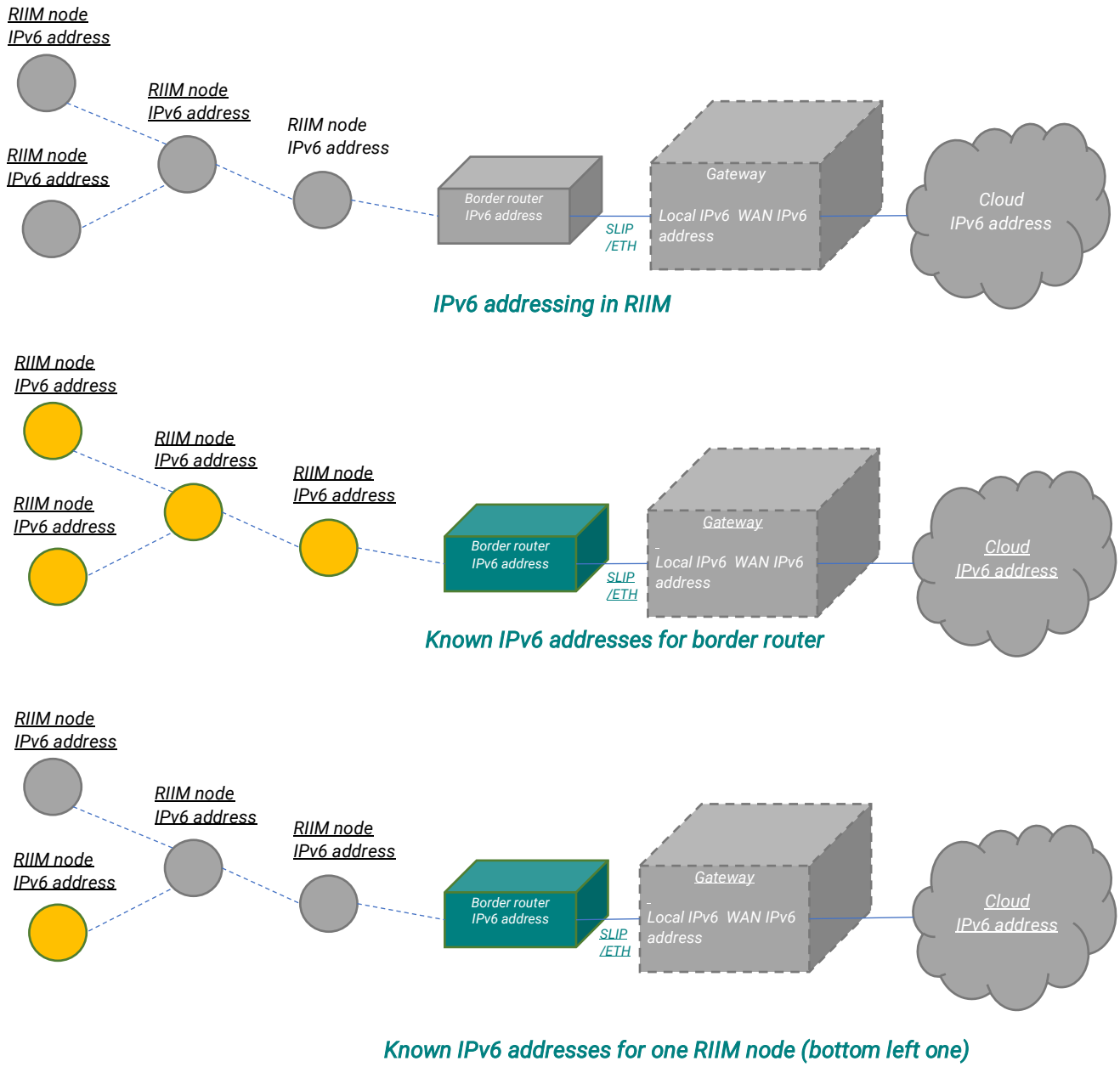


Figure 7. IPv6 addressing in RIIM

In cases where communication is only from a node to the border router or from the border router one or more nodes, the devices discovery is easy as it is automatically handled in RIIM.
But for more complex networks, then there are many other use cases in which one node needs to find the IP address of other devices. All possible use cases are covered in Table 1.

Device to be discovered / Device discovering	Cloud	Gateway	Border router	RIIM node
Cloud		Not really feasable to do direct. The device discovey of the gateway always need to be initiade from the gateway that registers itself at the cloud service.	Not really feasable to do direct. The device discovey of the border router always need to be initiade from the border router that registers itself at the cloud service.	Not really feasable to do direct. The device discovey of the RIIM node always need to be initiade from the RIIM node that registers itself at the cloud service.
Gateway	The initial address to the cloud service can be hard-coded in the gateway or found through DNS lookup		Since the BR knows the IPv6 address of the GW, it can register itself on the GW.	RIIM supports this nativly out of the box
Border router	Can be hardcoded in border router or discover by quering this address from gateway	If using SLIP: The local IPv6 address of the GW is normally hardcoded in gateway and can then be hardcoded in border router. If using ethernet: The IP address of the gateway needs to be set out-of-band in border router.		RIIM supports this nativly out of the box
RIIM node	Cloud address typically queried from gateway or border router	Gateway address typically queried from border router	RIIM supports this nativly out of the box	

Table 1. Use cases for device discovery in RIIM

The use cases in Table 1 show that even though device A cannot find device B, this can be fixed if device B can find device A and then register itself by sending a message to device A. This way device A gets the IP-address of device B and can thereafter store this and address device B.

Service Discovery

Service dicovery is one of the key aspects of nodes commissioning, but only relevant to network where node have different functions. If all nodes in the network are identical and offers the same "services" then this point is not required.

Service discovery refers to the process by which the Border Router (and possibly the cloud) maps the nodes IDs (in RIIM™ IPv6 addresses are used) to the real locations or functons of nodes. This is used when the application running in the gateway or cloud needs to use the information from nodes to take action.

Let's consider a simple IAQ (Indoor Air Quality) system as an example. Assume there is a sensor in each office room. If the air in the meeting room turns poor (High temperature, high humidicy, or high CO_2 concentration), then the ventilation for this room needs to be adjusted.

So somehow the central system must know the address of the sensor in the meeting room and map this to ventilation for this room.

Mapping IP addresses to functions or physical device will be various in different use cases and covering all in detail is out of scope for this application note, however there are several methods that can be used.

- *Serial number (physically printed on then product and stored electronically)*
  - *This application can read the serial number and send it to central location*
- *Button*
  - *"Identify" button that sends a message to the central system when pushed*
- *Visual signaling (e.g., blinking LED)*
  - *Central system can send a message to an IPv6 address and ask it to identify itself.*
  - *This can result in a LED blinking for e.g., 1 minute.*
- *Barcode + external tool*
  - *External tool can be used to scan barcode on product, and they can then manually in tool be set to physical location or function*
- *GPS*
  - *Outdoor systems can use GPS to identify location of nodes*

Summary

Correct and safe nodes commissioning is crucial for the network's safety and operation. Commissioning can encompass a number of aspects of a network setup, such as; network formation, device discovery, and service discovery. Numerous ways exist to commission a network, with each technology provider offering their available commissioning options according to what best suits that specific technology.

RIIM is based on IP and has inbuilt device discovery in the wireless network and through IP all devices can be identified, and all devices can be addressed.

This application notes focuses on the most used practices with RIIM™. It provides detailed explanation about the different aspects of commissioning a RIIM™ network. It also gives several alternatives to classical network formation methods, in addition to a brief explanation about services and device discovery with RIIM™.

Document Revision History

Document Revision	Changes
1.0.0	First release
1.1.0	Updated with section on commissioning collocated networks

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

RIIM™ is a trademark of Radiocrafts AS.

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.