SpaceWire PnP

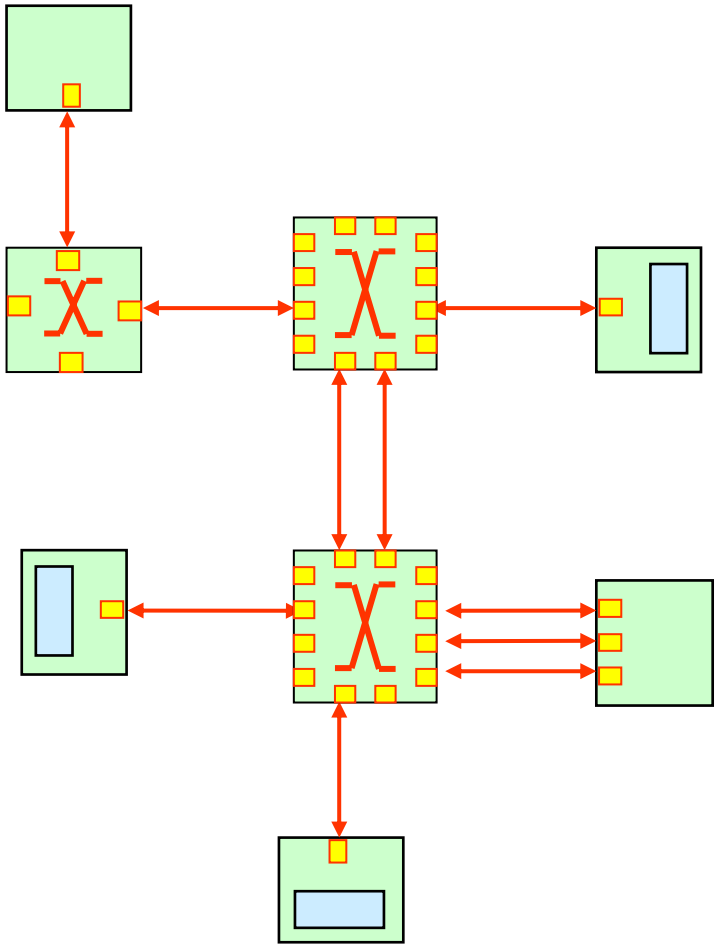
A software-Node based implementation

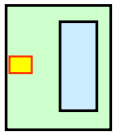
Albert Ferrer Florit
European Space Agency
TEC-EDP

Network Discovery

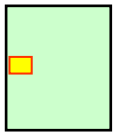
- Available routers implements one register dedicated to Network Discovery that can be accessed using RMAP.
- It provides information about the status of the ports and the number of input port used to access to this information.
- It also provides a General Purpose Register.
- It should be enough for a network discovery algorithm.

SpW Network Example





Node with a Processor unit with PnP algorithm



Node capable to process RMAP commands (RMAP slave)

Overview

- Plug ‘n’ Play (PnP) is implemented in software by some Intelligent nodes called Network Node Managers.
- A Network Node Manager (NNM) is a processor-based system programmed with a PnP algorithm.
- Each SpW region have one or more NNMs.
- Each router is configured by ONLY one NNM.
- NNMs read and configure router parameters using RMAP commands.
- NNMs communicate Network Information to other nodes using a dedicated SpW protocol ID.

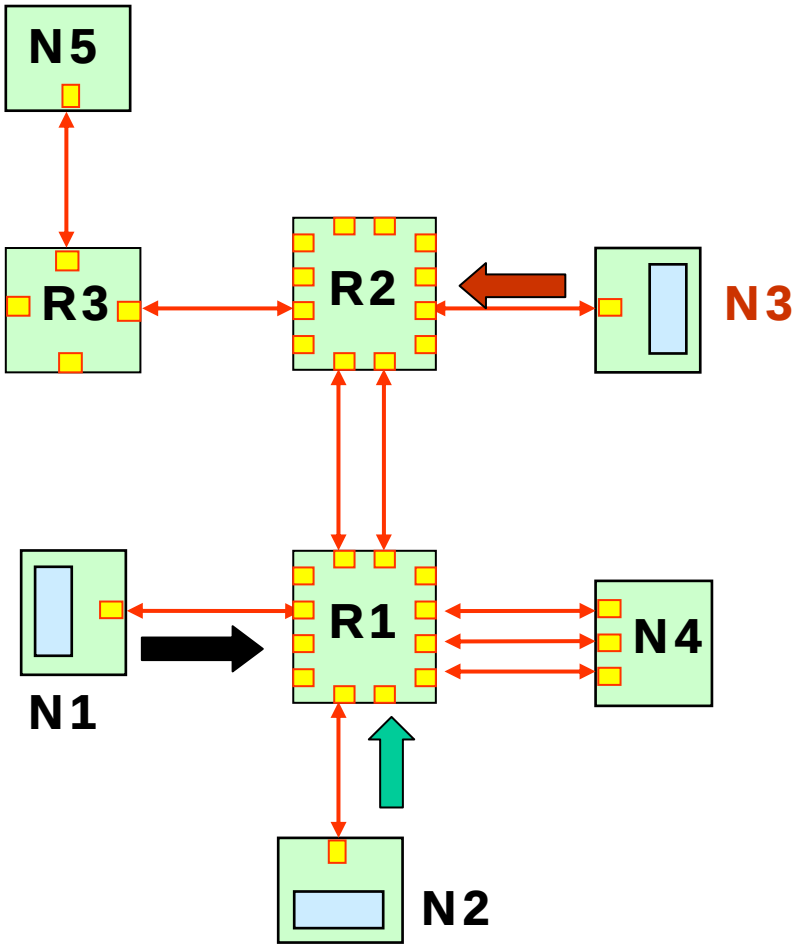
PnP algorithm objectives

- To detect if a port of a router is connected to a Node or to another router.
- To Obtain, at least, the Logical Address of all nodes connected to a router.
- If applicable, to configure the routing table and update it when a node is detached or attached.
- Provide network information to other nodes or NNMs.
- Implement redundancy and fault tolerant capabilities.
- Avoid RMAP blocking situations.

PnP algorithm - General Approach

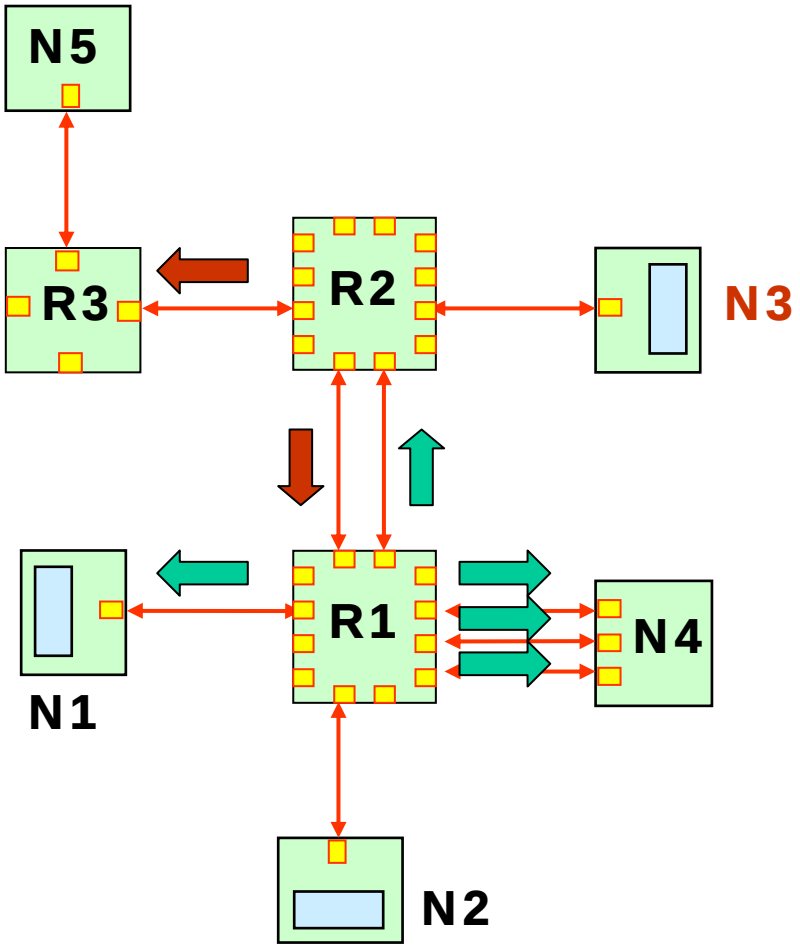
1) After reset each NNM reads the network discovery register of the router that it is attached to.
2) Each NNM read the General Purpose Register (GPR) of the router. If it contains no information then it writes its port number so other NNM that could be attached to the same router know who is responsible for this router.
3) Read again the register. (confirmation of ownership of the router)
4) Sends a read RMAP command with destination address 0 (configuration port) to all active ports of the router.
5) If another router is connected the reply will provide its network discovery register. If it is a node, it will provide its Logical Address.
6) If it is a router repeat points 2 and 3. If it is a node, try to identify it using a standard RMAP command or a specific PnP protocol ID.
7) If router belongs to another NNM, send available network information to the NNM using a specific PnP protocol ID.

PnP algorithm – Example (1)



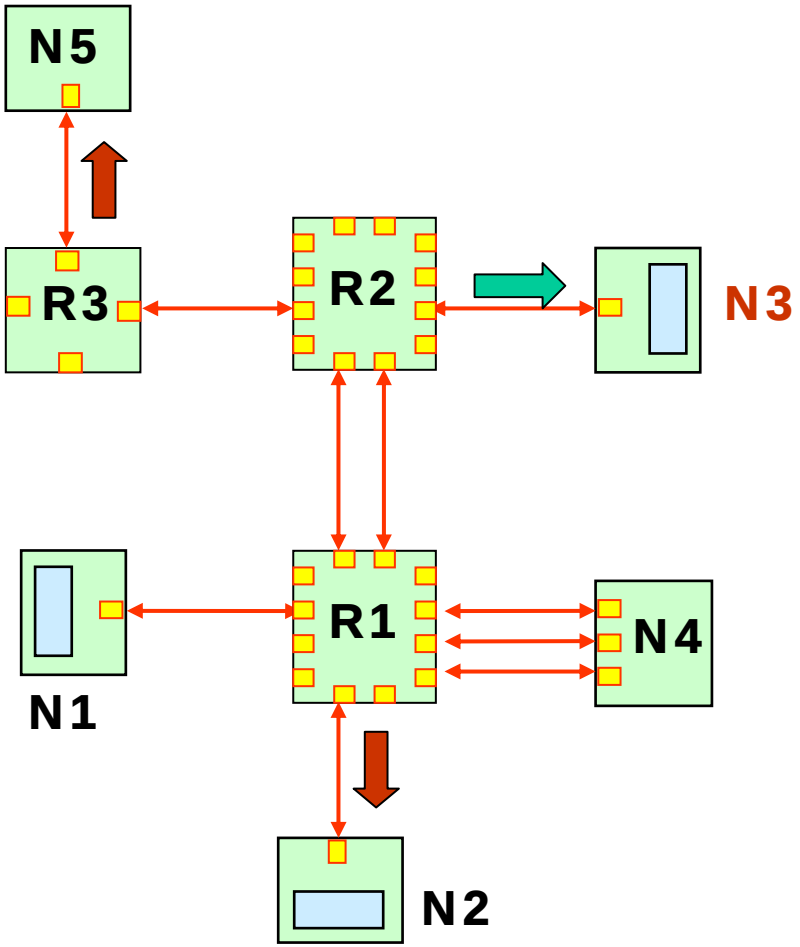
- N1,N2 reads network discovery register of router R1.
- N1,N2 writes its port number into the GPR register of R1
- N1,N2 check R1 GPR. N2 realise that N1 took control of the router first.
- N3 reads network discovery register of router R2.
- N3 writes its port number into the GPR register of R2.

PnP algorithm – Example (2)



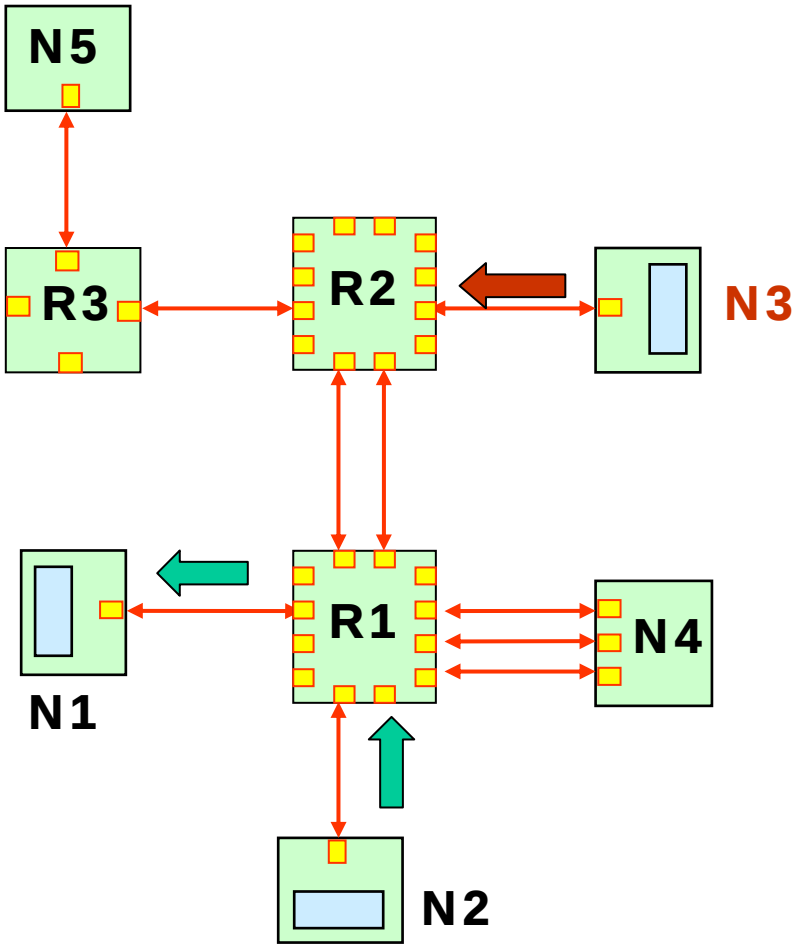
- N2,N3 send a read RMAP command with destination address 0 to all active ports of its router.
- N2 detects R2 and realise that another NNM has already taken control.
- N2 detects N1 and N4 and try to get their device information.
- N3 detects R3 and writes in its GPR the port number that has used to access it.
- N3 detects R1 and realise that another NNM has already taken control.

PnP algorithm – Example (3)



- N3 sends a read RMAP command with destination address 0 to all active ports of router R3
- N3 detects N5 and try to get their device information.
- N2 send a PnP packet to N3 using path addressing with information of R1 and its nodes attached.
- N3 send a PnP packet to N2 using path addressing with information of R2 and R3 and their nodes attached.

PnP algorithm – Example (4)



- N3 updates R2, R3 routing tables.
- N2 updates R1 routing table and send network status to N1.
- N2,N3 Periodically read status of their routers.

Note: Network status can contain device identification information including NNM capability. This can be used to optimise and supervise the NNM network.

PnP algorithm – Important issues

- A NNM should only access to a router through a link connected to a router that it has already taken control.
- Path addressing will be used to access to routers and send Network information between NNMs.
- Nodes should not send SpW packets until they have received the network configuration by NNMs.
- A master NNM can execute a complex routing algorithm and command other NNMs to implement the required routing tables.
- Therefore, most of the NNMs of the network will be used only to read/write router parameters, monitor their status and inform other NNMs of any change.

Conclusions (1)

- PnP capabilities can be implemented **with** the current **available SpW devices** by software means.
- It only requires that some nodes are programmed with a PnP Software algorithm.
- It avoids the RMAP blocking situation when reading router's parameters with RMAP.
- It is **redundant**, **scalable** and can implement **fault tolerant** capabilities.
- PnP algorithm does not make **any** assumption about the **topology** of the network.
- New passive nodes attached are always detected and can be identified if they implement a standard RMAP device ID register.
- **Traffic** related to monitor the network is **minimised**.

Conclusions (2)

In order to easily identify any node, SpW community should standardize a RMAP command for the network discovery with:

(1) Default device identification registers.

(2) A default destination key to be able to access to them.

(3) A default Increment and Verified RMAP option.

The END

SpaceWire PnP

A software Implementation

DRAFT A

Albert Ferrer Florit
European Space Agency (TEC-EDP)

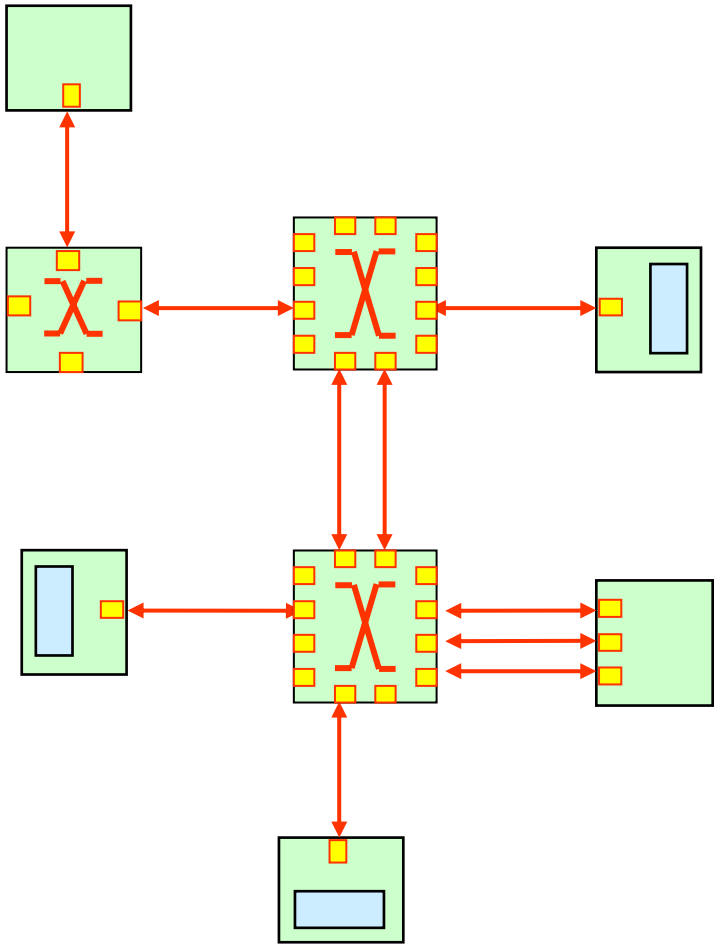
Overview

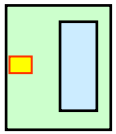
- Plug ‘n’ Play (PnP) is implemented in software by some Intelligent nodes called Network Node Managers.
- A Network Node Manager (NNM) is a processor-based system programmed with a PnP algorithm.
- Each SpW region have one or more NNMs.
- Each router is configured by ONLY one NNM.
- NNMs read and configure router parameters using RMAP commands.
- NNMs communicate Network Information to other nodes using a dedicated SpW protocol ID.

Requirements

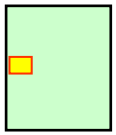
- All nodes and routers should be able to reply RMAP commands.
- Routers should provide information about the status of their ports.
- Processor-based nodes should be able to process packets with a SpW ID protocol reserved for PnP purpose.
- It is recommended that by means of RMAP a NNM can identify any device. A standard register address and destination key should be defined for this purpose.

SpW Network Example





Node with a Processor unit with PnP algorithm



Node capable to process RMAP commands (RMAP slave)

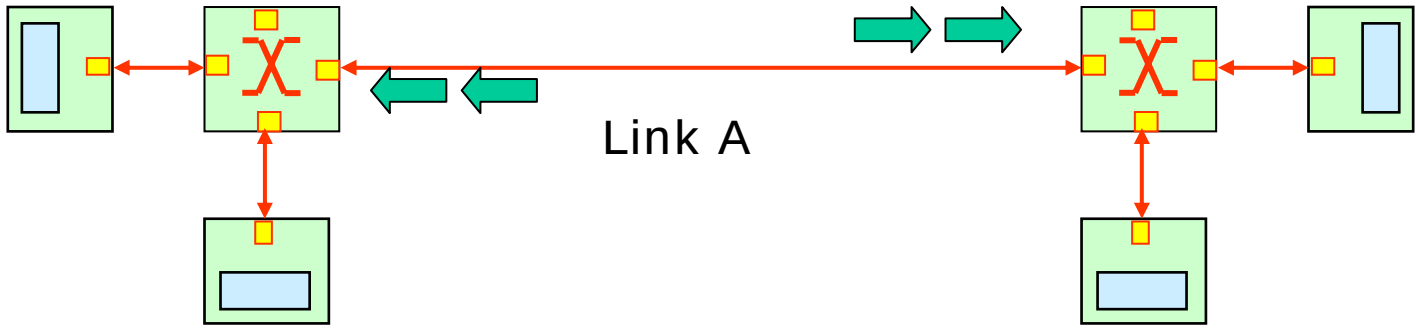
Network Discovery

- UoD router implements one register dedicated to Network Discovery that can be accessed using RMAP.
- It provides information about the status of the ports and the number of input port used to access to this information.
- It also provides a General Purpose Register.
- It should be enough for a network discovery algorithm.

PnP algorithm objectives

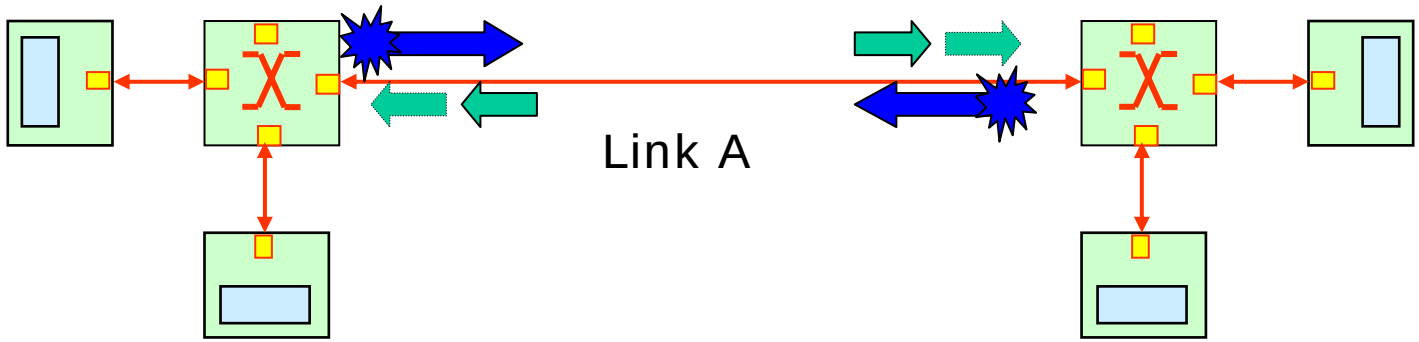
- To detect if a port of a router is connected to a Node or to another router.
- To Obtain, at least, the Logical Address of all nodes connected to a router.
- If applicable, to configure the routing table and update it when a node is detached or attached.
- Provide network information to other nodes or NNMs.
- Implement redundancy and fault tolerant capabilities.
- Avoid RMAP blocking situations.

RMAP blocking (1)



- All nodes tries to read both router parameters at the same time (i.e. after reset). First, they access the router where they are connected. Then they try to access the router that is connected to the first one accessed.
- It is possible that each router receives at the same time two consecutive read commands at each side of the link A

RMAP blocking (2)

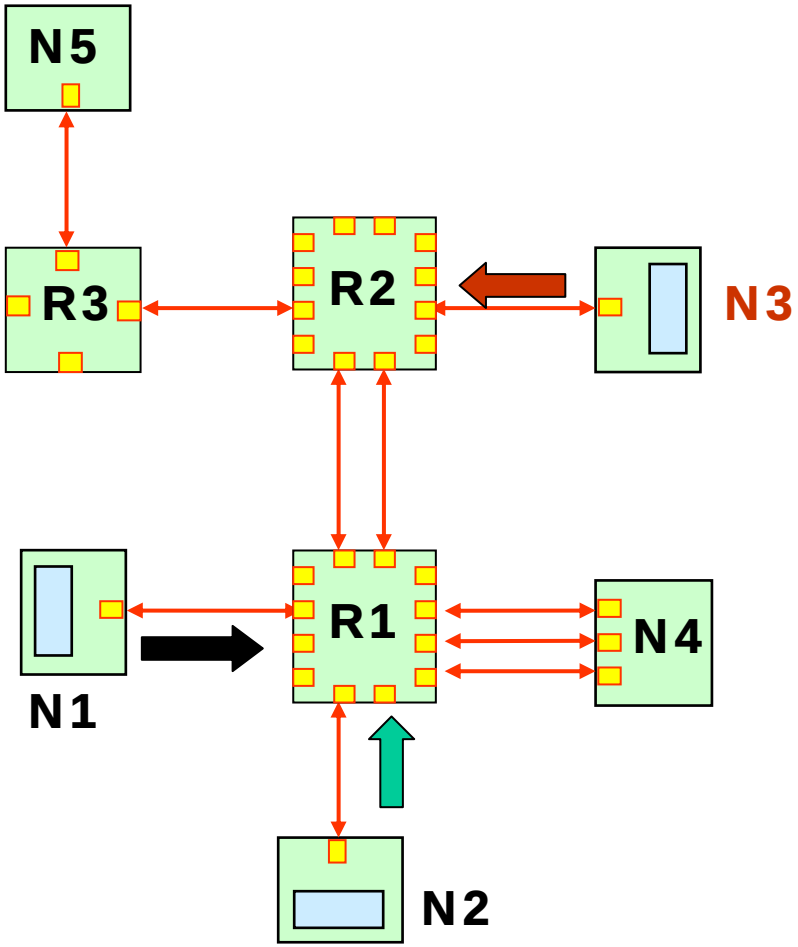


- A RMAP read command is processed and a reply is generated in each router.
- However, read replies can not be sent because are blocked by the other read commands that are waiting to be processed.
- A PnP algorithm that read router's status using RMAP should avoid this situation.

PnP algorithm - General Approach

1) After reset each NNM reads the network discovery register of the router that it is attached to.
2) Each NNM read the General Purpose Register (GPR) of the router. If it contains no information then it writes its port number so other NNM that could be attached to the same router know who is responsible for this router.
3) Read again the register. (confirmation of ownership of the router)
4) Sends a read RMAP command with destination address 0 (configuration port) to all active ports of the router.
5) If another router is connected the reply will provide its network discovery register. If it is a node, it will provide its Logical Address.
6) If it is a router repeat points 2 and 3. If it is a node, try to identify it using a standard RMAP command or a specific PnP protocol ID.
7) If router belongs to another NNM, send available network information to the NNM using a specific PnP protocol ID.

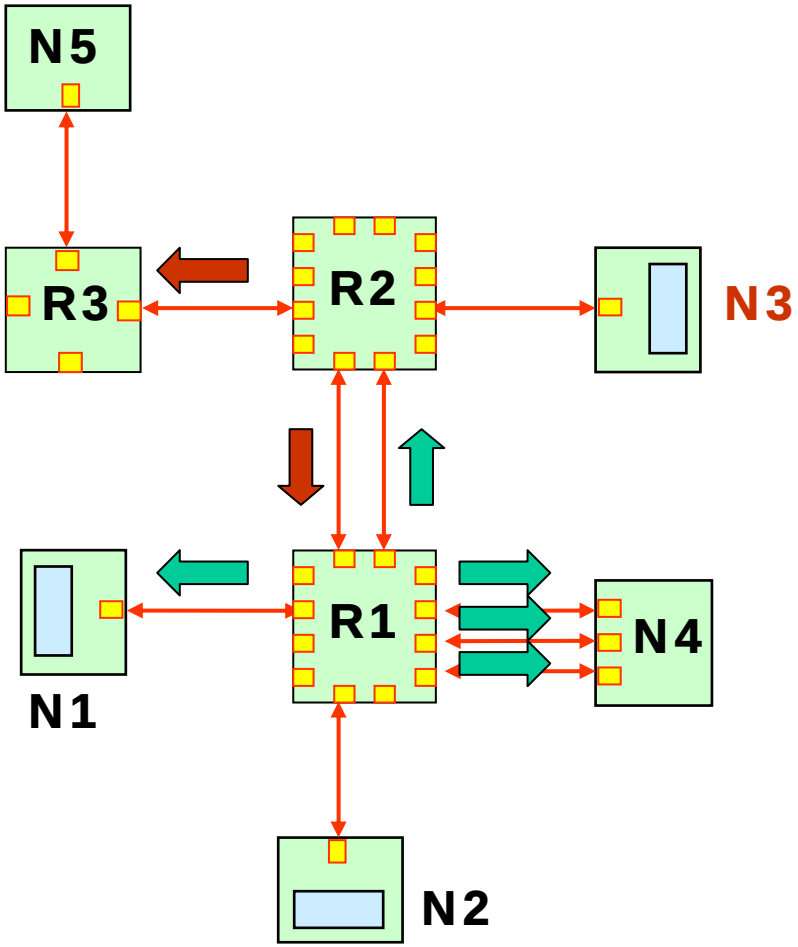
PnP algorithm – Example (1)



After Reset

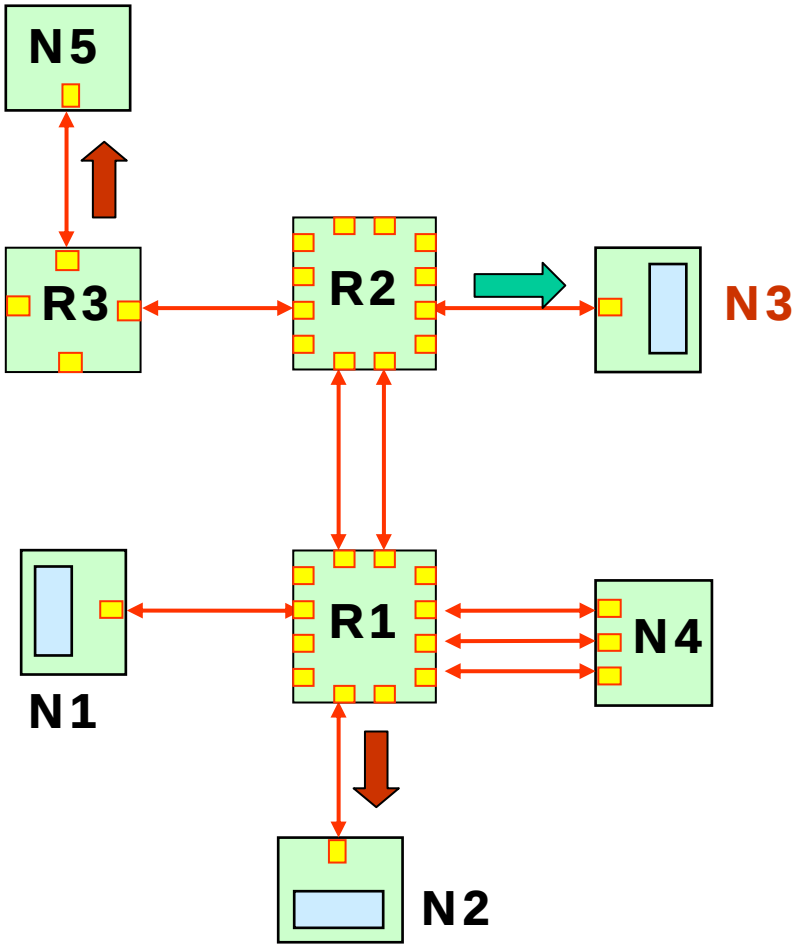
- N1,N2 reads network discovery register of router R1.
- N1,N2 writes its port number into the GPR register of R1.
- N1,N2 check R1 GPR. N2 realise that N1 took control of the router first.
- N3 reads network discovery register of router R2.
- N3 writes its port number into the GPR register of R2.

PnP algorithm – Example (2)



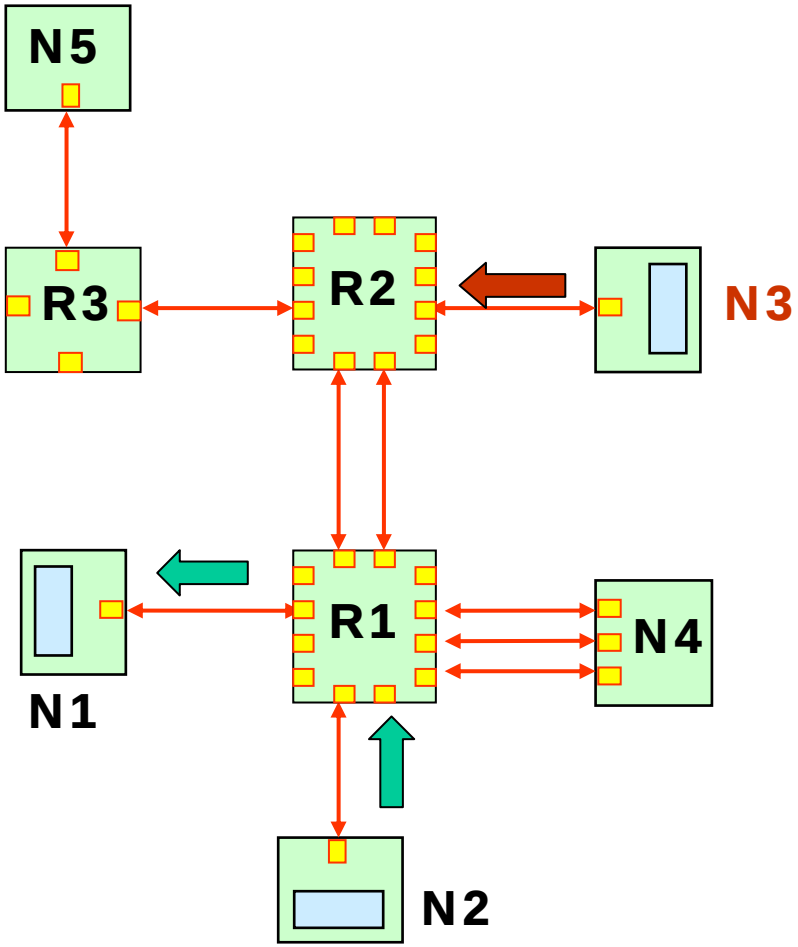
- N2,N3 send a read RMAP command with destination address 0 to all active ports of its router.
- N2 detects R2 and realise that another NNM has already taken control.
- N2 detects N1 and N4 and try to get their device information.
- N3 detects R3 and writes in its GPR the port number that has used to access it.
- N3 detects R1 and realise that another NNM has already taken control.

PnP algorithm – Example (3)



- N3 sends a read RMAP command with destination address 0 to all active ports of router R3
- N3 detects N5 and try to get their device information.
- N2 send a PnP packet to N3 using path addressing with information of R1 and its nodes attached.
- N3 send a PnP packet to N2 using path addressing with information of R2 and R3 and their nodes attached.

PnP algorithm – Example (4)



- N3 updates R2 routing table.
- N2 updates R1 routing table and send network status to N1.

Note: Network status can contain device identification information including NNM capability. This can be used to optimise the NNM network

PnP algorithm – Hot attachment

1)Each NNM periodically checks the port status of the routers that controls.

2)When a new active port is detected, it tries to read the device information using RMAP and PnP protocol ID.

3) NNM informs other NNMs and nodes of the new device detected and update routers tables if applicable.

4) If the new device is a processor based system it can announce its presence immediately to the NNM of the router that it is connected.

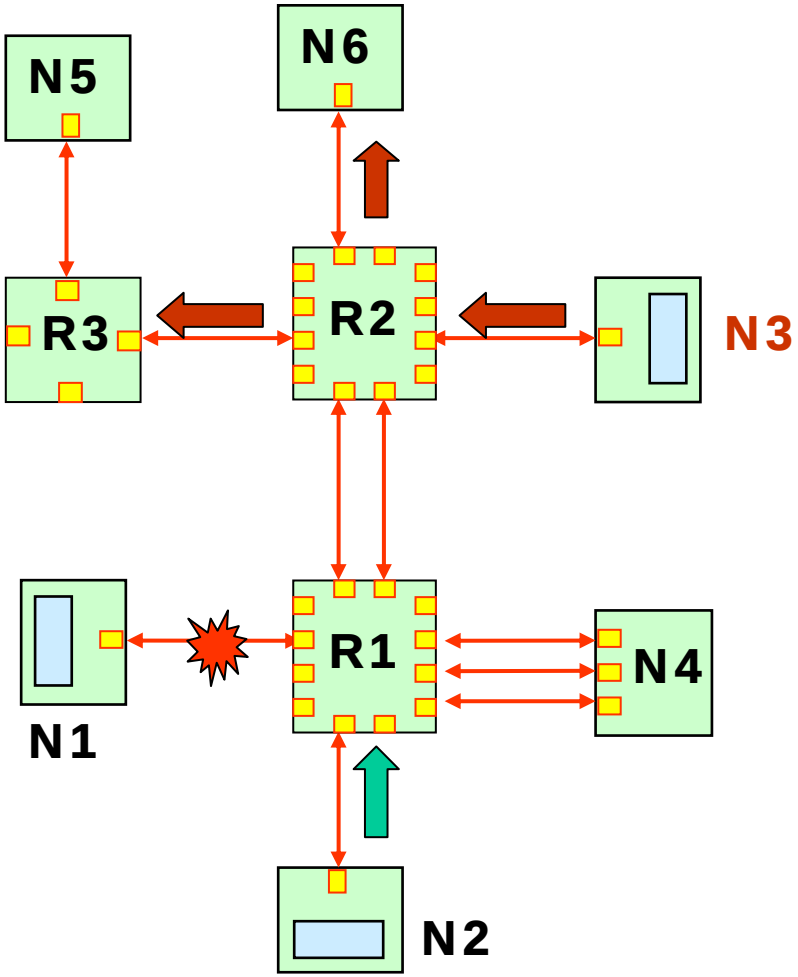
PnP algorithm – Hot detachments

1)Each NNM periodically check the port status of the routers that controls.

2)When a active port becomes inactive, NNM informs other NNMs and nodes of the new device detached and update routers tables if applicable.

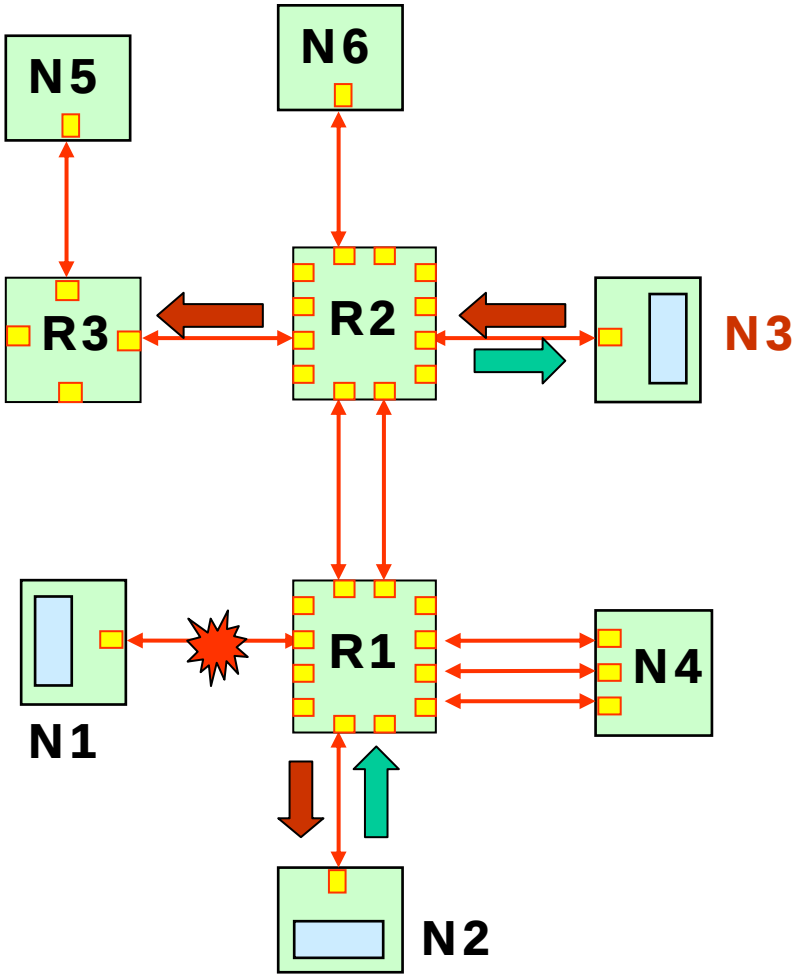
3) If a NNM receive a message that a device should be disconnected, it disconnects its port and informs other NNMs and nodes.

PnP algorithm – Example (5)



- N3 periodically read R2 and R3 status
- N3 detect that the new device N6.
- N2 periodically read R1 status
- N2 detects that N1 link stopped working

PnP algorithm – Example (6)



- N2 informs N3 of detachment of N1
- N3 informs N2 of the new device N6
- N3 update routing table of R2,R3
- N2 update routing table of R1
- N2,N3 keep monitoring R1,R2 and R3.
- N2,N3 exchange periodical status messages.

PnP algorithm – Important issues

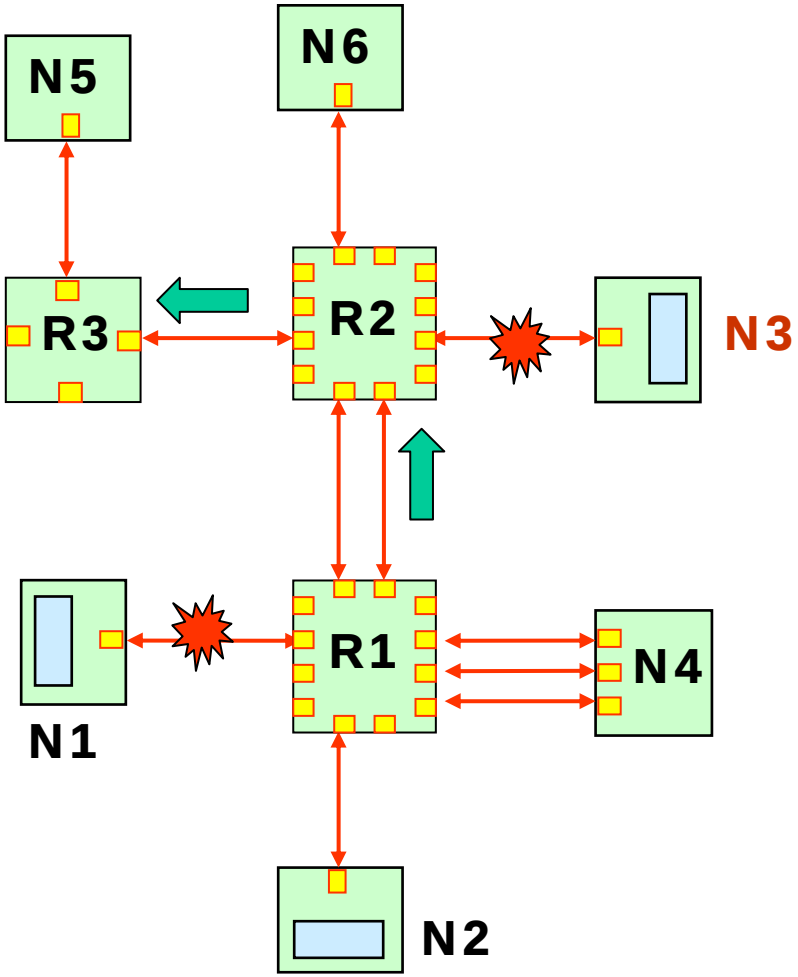
- A NNM should only access to a router through a link connected to a router that it has already taken control.
- Path addressing will be used to access to routers and send Network information between NNMs.
- Nodes should not send SpW packets until they have received the network configuration by NNMs.
- A master NNM can execute a complex routing algorithm and command other NNMs to implement the required routing tables.
- Therefore, most of the NNMs of the network will be used only to read/write router parameters, monitor their status and inform other NNMs of any change.
- In this way the traffic related to monitor the network status is minimised.

PnP algorithm – Fault Tolerant

- A NNM will send periodically status information to its NNMs neighbours (using PnP Id protocol). If a NNM neighbour notification timeout then it will try to take control of the routers of the faulty NNM if there is no other closer inactive NNM available.

- If a node can not reach a destination it will notify it to the local NNM.

PnP algorithm – Example (6)



- N3 fails.
- N2 stop receiving status messages from N3.
- N2 tries to take control of all routers owned by N3.

PnP algorithm – Advantages

- It can be implemented with the current available SpW devices.
- It only requires that some nodes are programmed with a PnP Software algorithm.
- It avoids the RMAP blocking situation when reading router's parameters with RMAP.
- It is redundant, scalable and can implement fault tolerant capabilities.
- PnP algorithm does not make any assumption about the topology of the network.
- New passive nodes attached are always detected and can be identified if they implement a standard RMAP device ID register.
- Traffic related to monitor the network is minimised.

Conclusions

- PnP capabilities can be implemented with current SpW devices by software means.
- The proposed solution avoids RMAP blocking situations, is redundant, scalable and fault tolerant.
- Traffic related to monitor the network can be minimised by adding more network node managers.
- In order to easily identify any node, SpW community should standardize default device identification registers and a default destination key to be able to access to them.