Monday 2022/06/27

IETF ROLL interim - online

Routing over Low-Power And Lossy Networks

Chairs:

Dominique Barthel

Ines Robles

Secretary:

Michael Richardson

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)

Note Well

•IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need to confidentially raise concerns about harassment or other conduct in the IETF.

•The IETF strives to create and maintain an environment in which people of many different backgrounds are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.

•IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior -- in particular, speech or behavior that is aggressive or intimidates.

•If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

Source: https://www.ietf.org/about/note-well/

Meeting Materials

- Remote Participation
  - Meetecho: https://meetings.conf.meetecho.com/interim/?short=2c2aafd8-db44-4245-b7f8-b671c19ba084
  - Material: https://datatracker.ietf.org/meeting/interim-2022-roll-01/session/roll
  - Jabber: xmpp:roll@jabber.ietf.org?join
  - CodiMD: https://codimd.ietf.org/notes-ietf-interim-2022-roll-01-roll
  - Minute takers: **Please volunteer, thank you :)**

Agenda

IETF - ROLL Interim

Monday, 27th June 2022 - From 14:00 to 15:30 UTC

Material: https://datatracker.ietf.org/meeting/interim-2022-roll-01/session/roll

Notes: https://notes.ietf.org/notes-ietf-interim-2022-roll-01-roll

Time	Duration	Draft/Topic	Presenter
14:00 - 14:10	10 min	WG Status	Ines/Dominique
14:10 - 14:25	15 min	draft-ietf-roll-aodv-rpl	Charlie
14:25 - 14:40	15 min	draft-ietf-roll-dao-projection	Pascal
14:40 - 14:55	15 min	draft-ietf-roll-rnfd	Konrad
14:55 - 15:00	5 min	Open Floor	Everyone

State of Active Internet-Drafts

Common Ancestor Objective Function and Parent Set DAG Metric Container Extension draft-ietf-roll-nsa-extension-10	AD evaluation, revised I-D needed
Supporting Asymmetric Links in Low Power Networks: AODV-RPL draft-ietf-roll-aodv-rpl-13	Back to the WG Short discussion today
Root initiated routing state in RPL draft-ietf-roll-dao-projection-26	Discussed today To be WGLC'ed
Controlling Secure Network Enrollment in RPL Networks draft-ietf-roll-enrollment-priority-06	Discussed today
Mode of Operation extension draft-ietf-roll-mopex-04	waiting for attention (expired Nov 2021)
RPL Capabilities draft-ietf-roll-capabilities-09	waiting for attention (expired Nov 2021)
RPL Storing Root-ACK draft-jadhav-roll-storing-rootack-03	WG adoption to be called
RNFD: Fast border router crash detection in RPL draft-ietf-roll-rnfd-00	New Work adopted by the WG

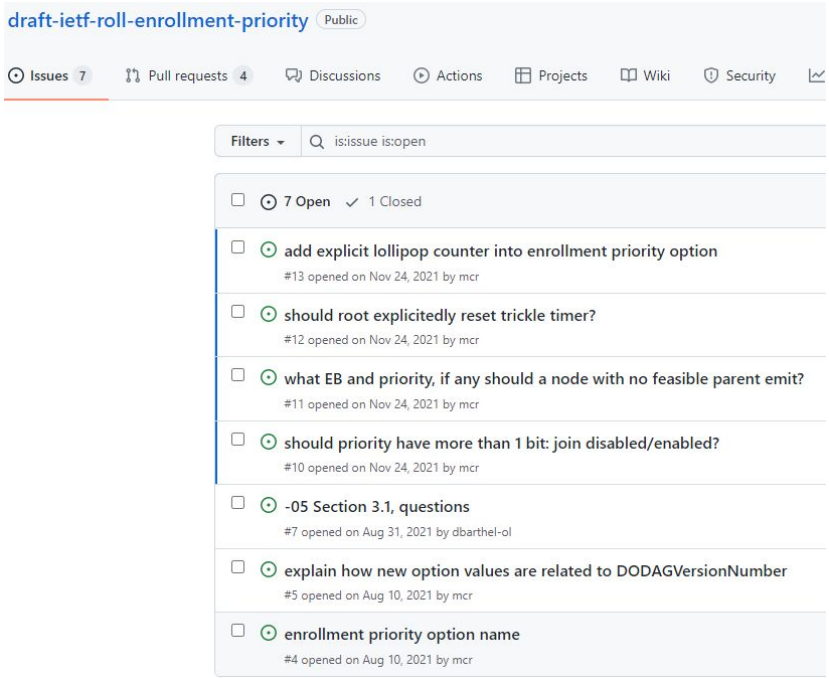
Inactive WG Internet-Drafts

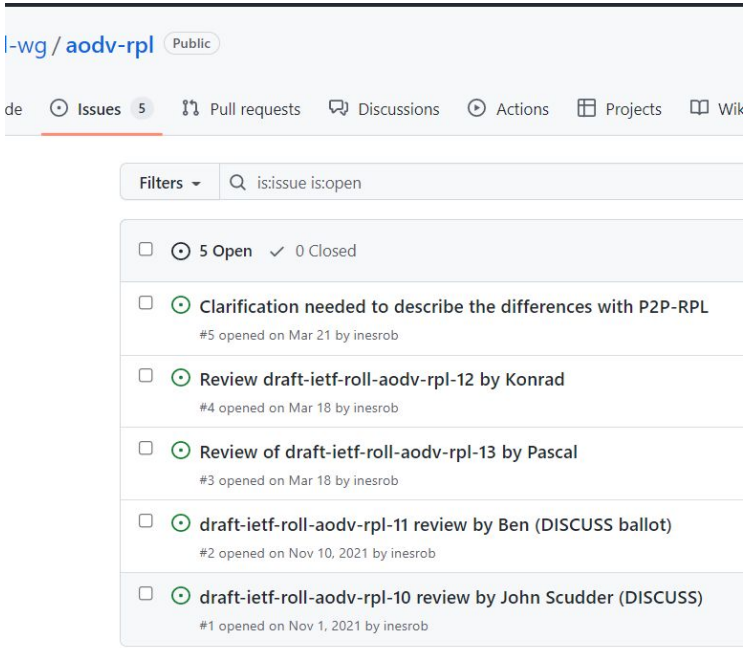
Draft	Status
RPL DIS modifications draft-ietf-roll-dis-modifications	Expired, waiting for attention
Draft-ietf-roll-mpl-yang-02	Long expired, dormant
Draft-ietf-roll-bier-ccast-01	Long expired, dormant

Milestones

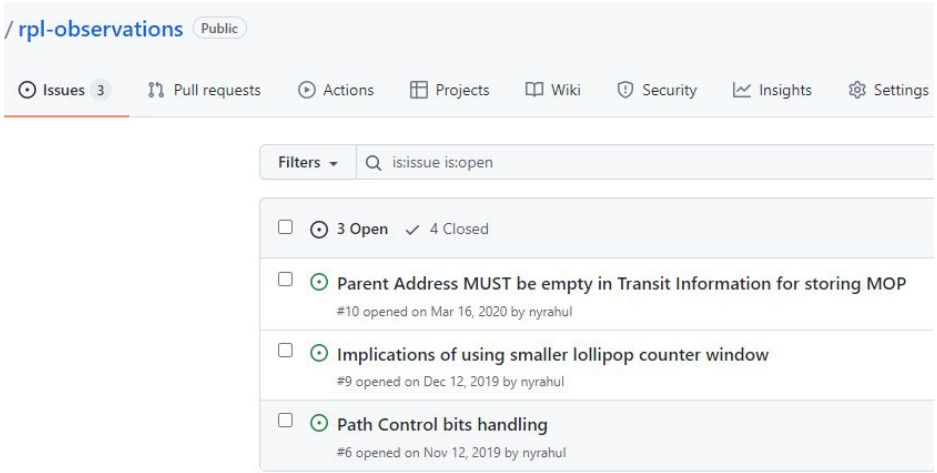
Initial submission of Root initiated routing state in RPL to the IESG (draft-ietf-roll-dao-projection)	May 2022
Initial submission of Controlling Secure Network Enrollment in RPL networks to the IESG draft-ietf-roll-enrollment-priority	Sep 2022
Initial submission of Mode of Operation extension for RPL to the IESG (draft-ietf-roll-mopex)	Nov 2022
Initial submission of Capabilities for RPL to the IESG (draft-ietf-roll-capabilities)	Jun 2023
Initial submission of RNFD: Fast border router crash detection in RPL to the IESG (draft-ietf-roll-rnfd)	Nov 2023
Initial submission of a proposal to augment DIS flags and options to the IESG draft-ietf-roll-dis-modifications	Nov 2023
Recharter WG or close	Nov 2023
Initial submission of YANG model for MPL to the IESG (draft-ietf-roll-mpl-yang)	Nov 2023
Initial submission of a proposal for Source-Route Multicast for RPL to the IESG (draft-ietf-roll-ccast)	Nov 2023

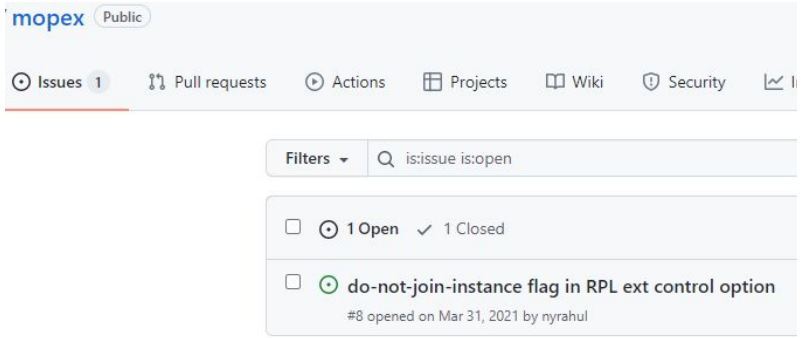
Open Tickets





Open Tickets





IETF 114 Preliminary Agenda (UTC)

20:00-21:00	Thursday Session III			
	Independence C	art	extra	Email mailstore and eXtensions To Revise or Amend
	Liberty C	gen	shmoo	Stay Home Meet Occasionally Online
	Liberty B	int	madinas	MAC Address Device Identification for Network and Application Services
	Liberty D	rtg	mpls	Multiprotocol Label Switching
	Philadelphia South	rtg	roll	Routing Over Low power and Lossy networks
	Philadelphia North	sec	acme	Automated Certificate Management Environment
	Independence A/B	sec	privacypass	Privacy Pass
	Freedom E/F	sec	suit	Software Updates for Internet of Things

14:00-16:00	Friday Session I			
	Philadelphia South	art	httpapi	Building Blocks for HTTP APIs
	Philadelphia North	irtf	panrg	Path Aware Networking RG
	Liberty C	ops	mops	Media OPerationS
	Independence A/B	ops	opsawg	Operations and Management Area Working Group Combined OpsAWG/OpsAREA
	Independence C	rtg	ccamp	Common Control and Measurement Plane
	Freedom E/F	rtg	manet	Mobile Ad-hoc Networks Joint MANET/BABEL/ROLL
	Liberty B	rtg	pals	Pseudowire And LDP-enabled Services
	Liberty D	sec	oauth	Web Authorization Protocol
16:00-16:30	Liberty Ballroom Foyer			Beverage and Snack Break

Supporting Asymmetric Links in Low Power Networks: AODV-RPL

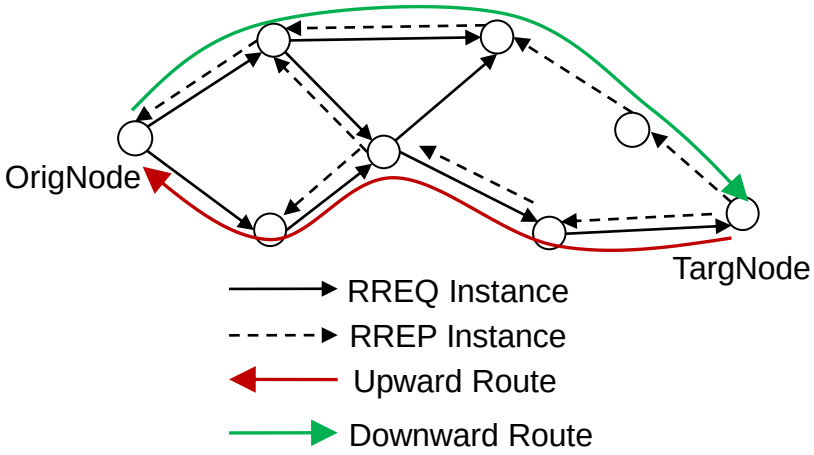
draft-ietf-roll-aodv-rpl-14

Interim [roll] WG meeting, June 27, 2022

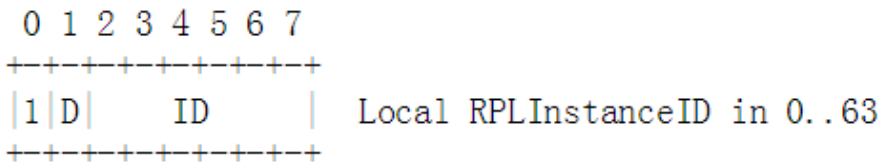
Charlie Perkins <charles.perkins@earthlink.net>
S.V.R Anand <anand@ece.iisc.ernet.in>
Satish Anamalamudi <satishnaidu80@gmail.com>
Mingui Zhang <zhangmingui@huawei.com>
Remy Liubing <remy.liubing@huawei.com>

AODV-RPL: Overview

- Differences with P2P-RPL
  - Two DODAGs rooted separately at the OrigNode and the TargNode
  - Support symmetric/asymmetric routes for upward and downward
  - Higher route diversity in asymmetric thanks to decoupling constraints on two directions
  - Encapsulate RREQ and RREP of AODV into RPL Options
  - New multicast group all-AODV-RPL-nodes
  - RREQ sent by OrigNode, advertises a route to OrigNode, requests a route to TargNode
  - RREP sent by TargNode, advertises a route to TargNode, paired to RREQ previously sent by OrigNode
  - Enable gratuitous RREP
- Note: Bi-directional asymmetric link
  - Can be used in both directions for DIOs but the two directions may have different values for, e. g. bandwidth, latency



IPv6 RPL Option, RPLInstanceID



- RREQ Local Instance ID assigned by the OrigNode
- RREP Local Instance ID assigned by the TargNode
- Pairing the RREQ-instanceID and RREP-instanceID
  - multiple route discoveries possible between OrigNode and TargNode.
- If OrigNode's Instance ID is already used by TargNode
  - Shift it to another number (still between 0 and 63)
  - Recover OrigNode's according to the Delta field in RREP option

Changes from v13 to v14

- Provided more details about scenarios naturally supporting the choice of AODV-RPL as a routing protocol
- Added new informative references [RFC6687] & [RFC9010] that describe the value provided by peer-to-peer routing.
- Requested IANA to allocate a new multicast group to enable clean separation of AODV-RPL operation from previous routing protocols in the RPL family, even though still using MOP==4.
- Cited [RFC6550] as the origination of the definition of DIO
- Defined "hop-by-hop route" as a route created using RPL's storing mode.
- Defined new configuration variable REJOIN_REENABLE.
- RREQ-InstanceID=(RPLInstanceID, OrigNode_IPaddr)
- RREP-InstanceID=(RPLInstanceID, TargNode_IPaddr)

Changes from v13 to v14 (continued)

- Improved definition of source routing
- Clarified that the Border Router (BR) in "*Figure 4: AODV-RPL with Symmetric Instances*" doesn't imply that AODV requires a BR as a protocol entity.
- Provided more guidelines about factors to be considered by OrigNode when selecting a value for the 'L' field.
- Described the disadvantage of not keeping track of the Address Vector in the RREQ-Instance.
- Specified that in non-storing mode an intermediate node has to record the IP addresses of both incoming and outgoing interfaces into the Address Vector, when those interfaces have different IP addresses.
- Added three informative references to describe relevant details about evaluating link asymmetry.
- Clarified details about Gratuitous RREP.

Next Steps

- Last Call

Root initiated routing state in RPL

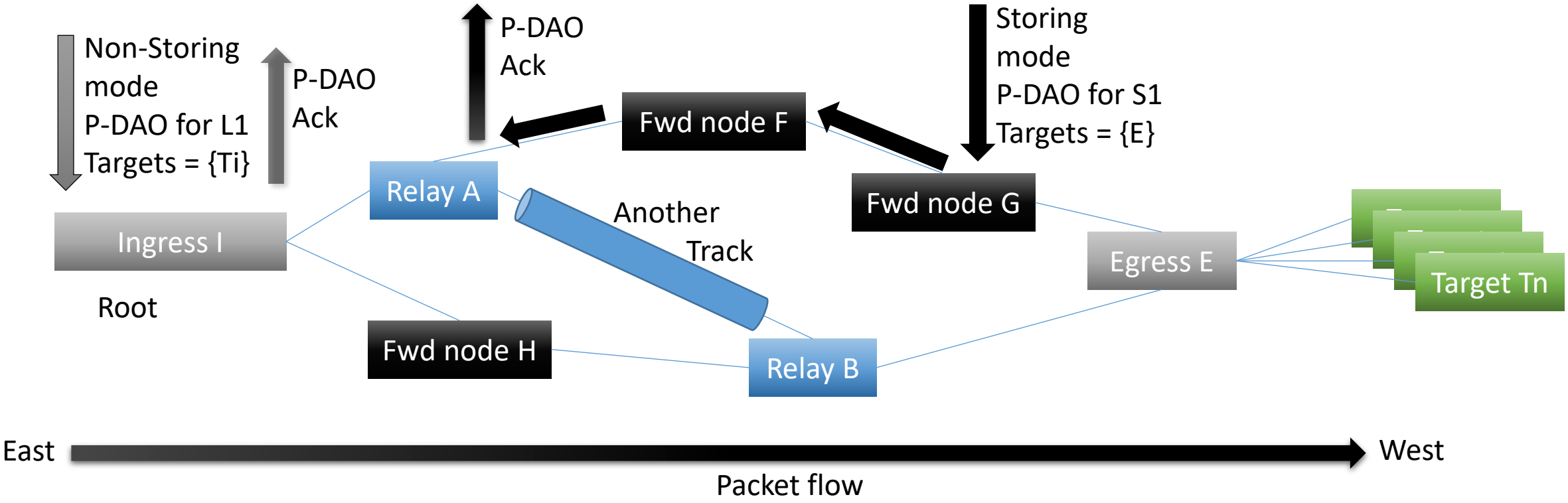
draft-ietf-roll-dao-projection

Pascal Thubert, Rahul Arvind Jadhav, Michael Richardson

Interim 01 / 2022

Presenter: Pascal Thubert, remote.

The RPL Track: A DODAG rooted at Ingress



Targets {Tx }

Legs L1 = I->A->E to {Ti} , L2 = I->B->E to {Ti} , L3 = I->A->B->E to {Ti}

Segments S1 = A=>F=>G to E , S2 = I=>H to B

SubTracks Any Set ⊂ {L1, L2, L3} but { }

Some rules

- Track is set up by installing Legs and Segment
  - with the same Track ID
- Non-Storing Mode P-DAO signals a Leg
- Storing Mode P-DAO signals a Segment
- Storing Mode P-DAO enables loose hops
  - in Non-Storing main DODAG (typically TrackId is Global instance ID)
  - in Tracks (typically TrackId is Local instance ID to track Ingress)
- Track Egress is implicit Target in Non-Storing Mode
- Leg hop is either a Segment of this Track or another Track

Status of the draft

- Latest rev is draft-ietf-roll-dao-projection-24
- 21: Includes IOT-DIR review by Toerless (before IETF 112)
- 22: Michael's review
- 23-24: Li's review
- 26: Remous-Aris' review
  - Clarifications, e.g., "A Track is typically an overlay to the main instance"
  - "the list of nodes in a VIO in Non-Storing Mode is exactly the list that shows in the encapsulation SRH"
  - Typos and language corrections (many)

Next

- WGLC; please consider:
  - Need for new status codes
  - Missing flows, e.g., Error flows

RNFD: Fast border router crash detection in RPL

draft-ietf-roll-rnfd-00

Adopted end of February 2022

Konrad Iwanicki

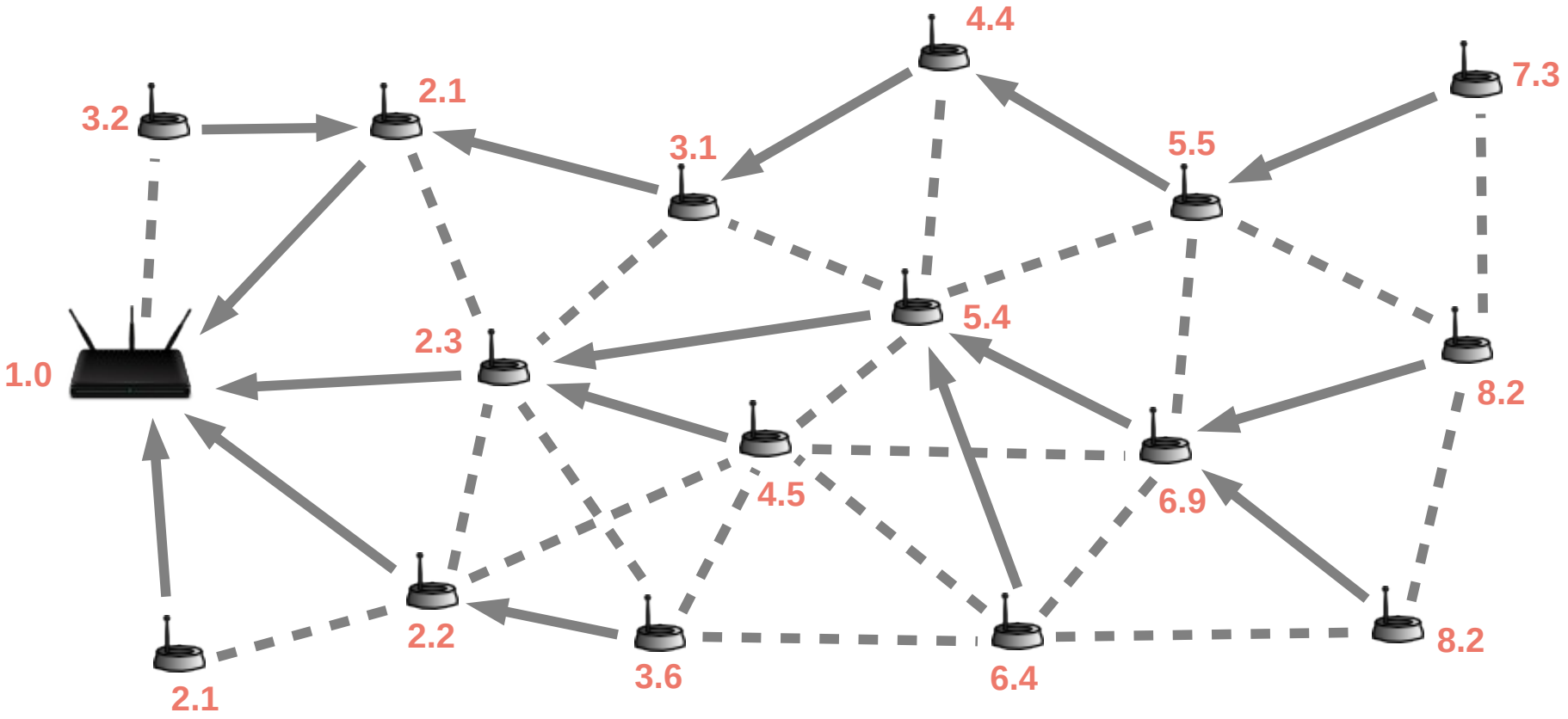
ROLL Interim, June 27th, 2022

Why consider LBR crashes?

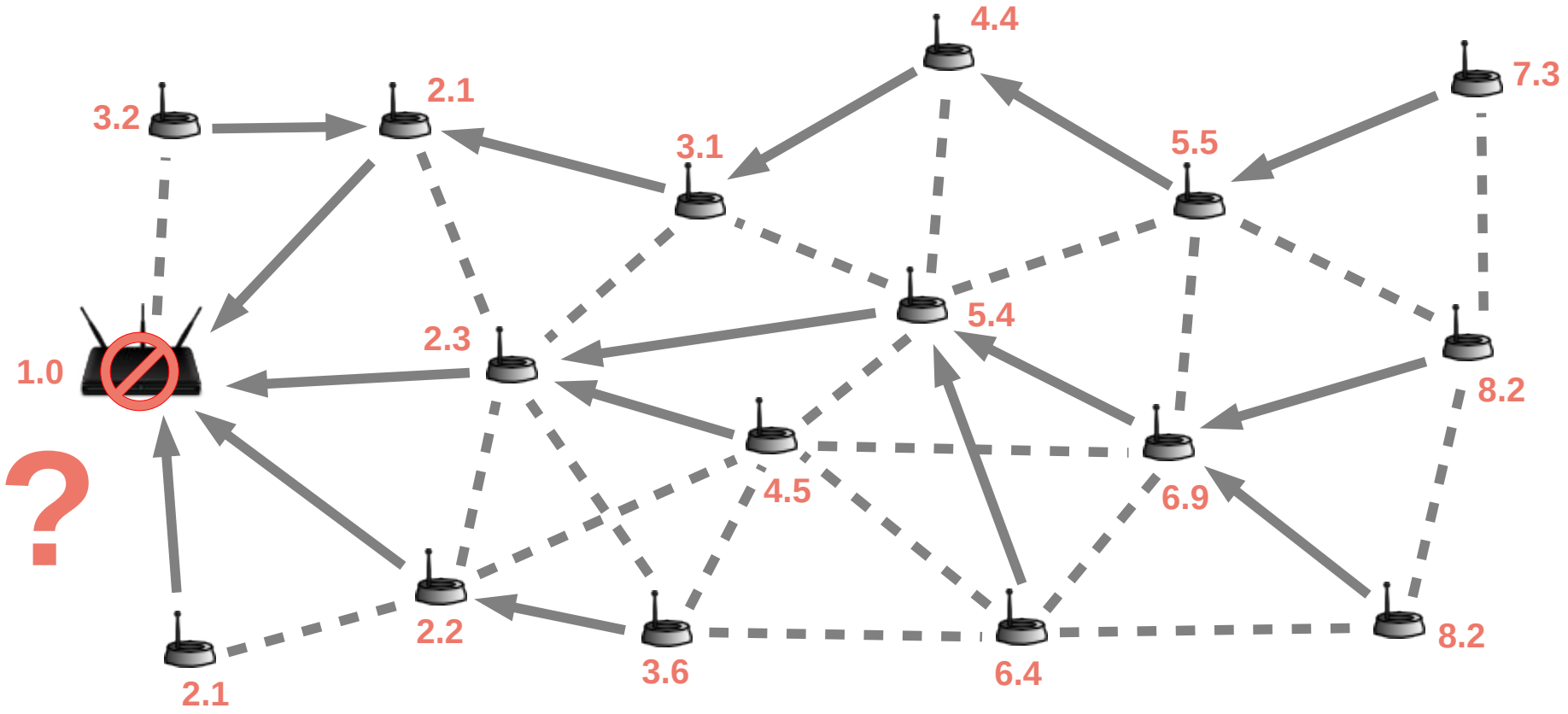
An LBR:

- plays a central role in an LLN (DODAG root),
- is typically more involved than a constrained node,
- usually requires a tethered power supply (hard to back up in many deployments).

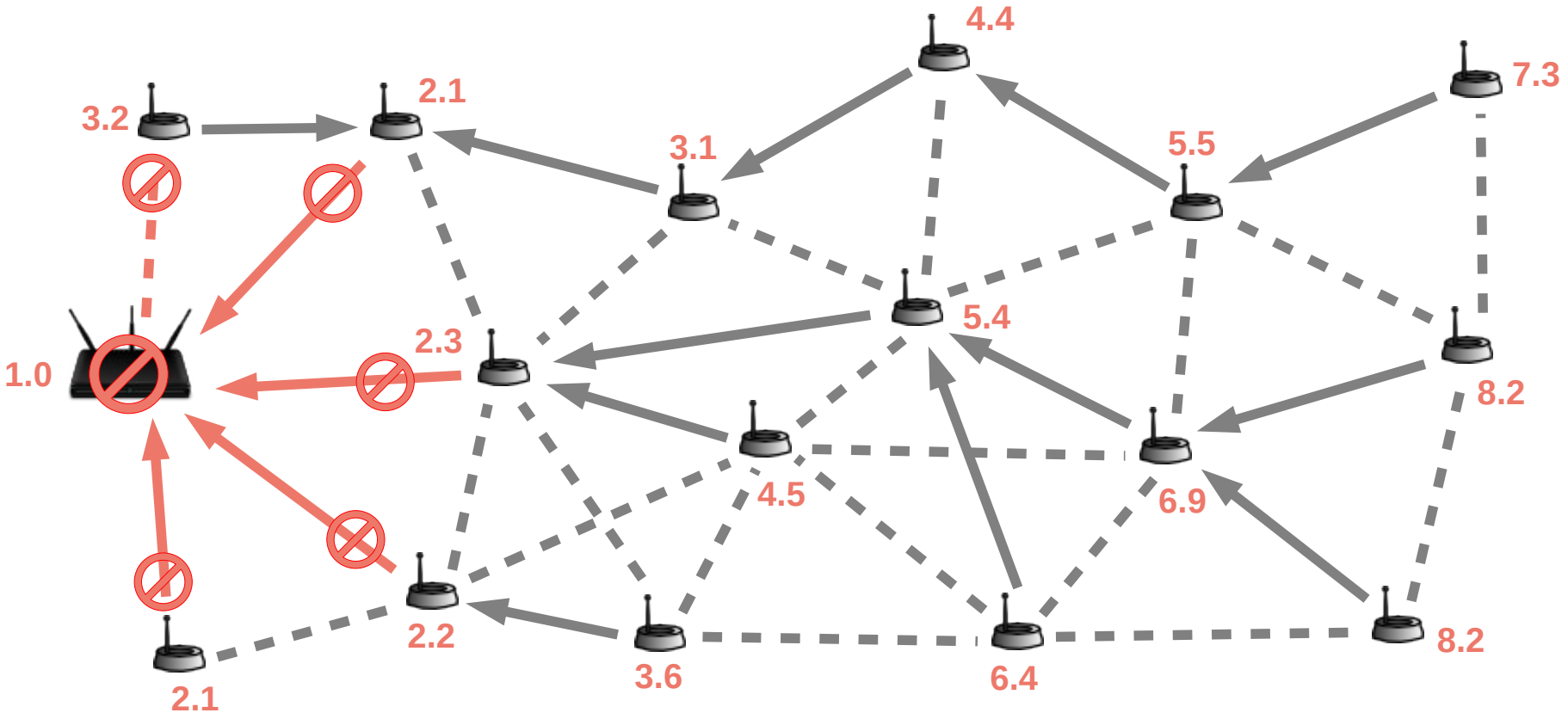
DODAG Root Failure in RPL



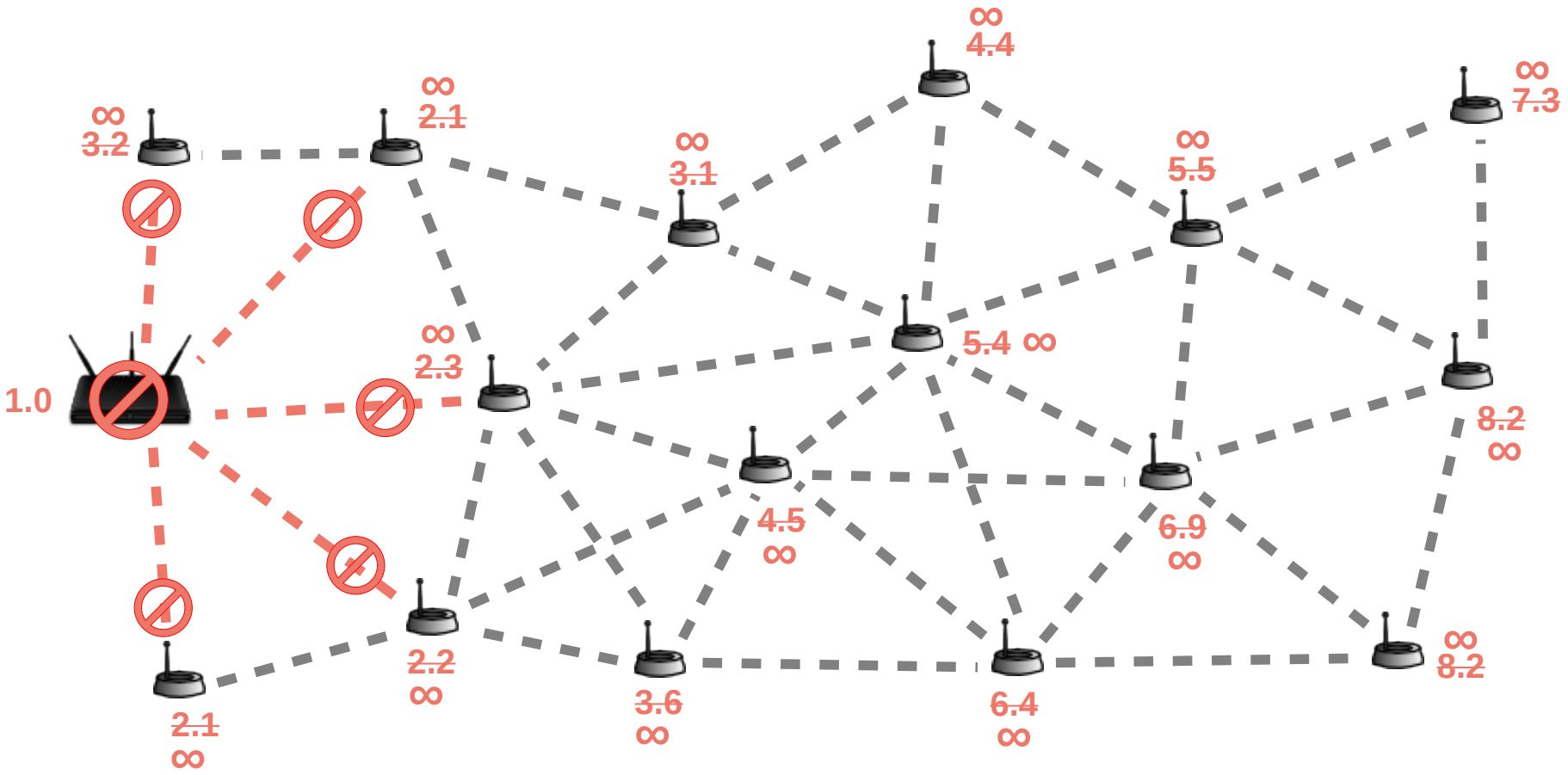
DODAG Root Failure in RPL



DODAG Root Failure in RPL



DODAG Root Failure in RPL



What happens in practice under an LBR crash?

- Some RPL stacks (with major bugs) enter a chaotic state in which an LLN simply collapses: explosion in control traffic.
- Some others (with minor bugs) do not detect the failure (in reasonable time): node ranks grow unbounded; control traffic is heavier than normally.
- Some are correct but still they require considerable:
  - time and
  - traffic.

  to handle an LBR crash.

What happens in practice under an LBR crash?

- All links to the dead LBR have to be detected as down by the LBR's neighbors.
  - Otherwise, the LBR's neighbor with such a link may incorrectly advertise a valid path.
- Link crash detection is typically reactive:
  - In low-data-rate applications, it may take a while.
- Learning by all nodes that none of their links may contribute to a path to the LBR is slow and requires traffic:
  - repeated parent changes due to local repair attempts,
  - routing loops due to inconsistencies between nodes,
  - Trickle timer resets upon parent changes and loop detection.

RNFD Goals

- RNFD = Root Node Failure Detector
- Goal: to minimize
  - time and
  - traffic

  required to detect a crash of an LBR (a DODAG root).
- Possible empirical improvements:
  - time = a few times, an order of magnitude less,
  - traffic = a few times less.

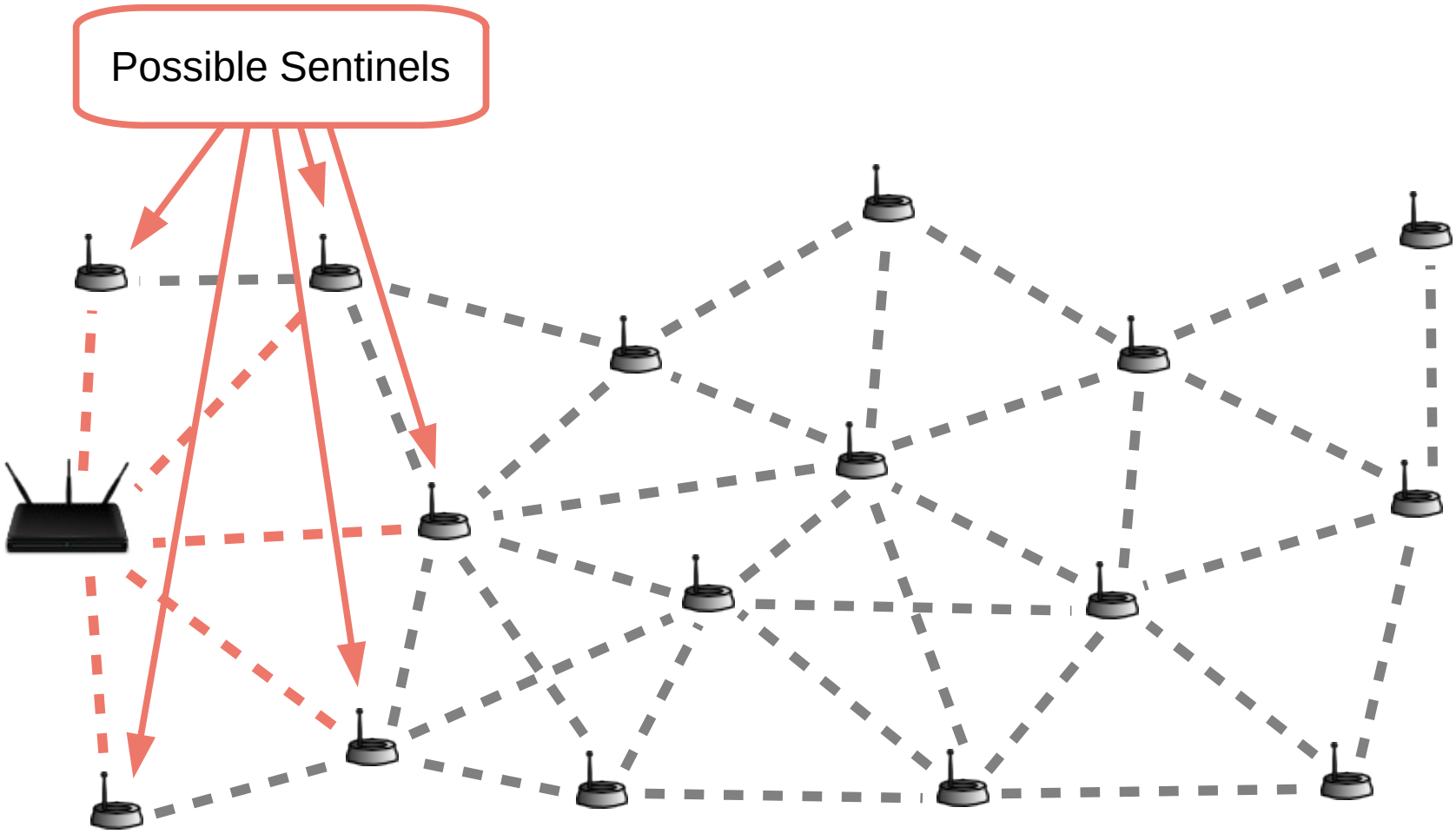
RNFD Design Principles

- Explicitly coordinating LBR monitoring between nodes.
- Avoiding probing all links to the dead LBR.
- Proactive checking for a possible LBR crash when some nodes suspect such a failure may have taken place.
- Maximizing independence of RPL.

Node Roles in RNFD

- Sentinel – DODAG root's neighbor that monitors the DODAG root's status.
  - There are typically multiple of them.
  - Not every neighbor of the root has to be Sentinel.
- Acceptor – any node that is not Sentinel and only accepts their observations.
  - The DODAG root itself is also Acceptor.

Node Roles in RNFD



Principal Ideas behind RNFD

- Individual sentinels detect crashes of their links to the DODAG root.
- This information is exchanged in a new option in link-local RPL messages (DIOs and DISs).
- Based on the number of sentinels having their links with the DODAG root down, all nodes consent that the DODAG root has crashed.

Status of the draft

- Adopted by the WG, after a fruitful discussion, at the end of February / beginning of March 2022:
  - The topic is important.
  - The solution need not be the final one.
- **Next steps?**
  - Michael’s suggestion: Adopt as is as Experimental Draft.
  - Pascal’s earlier remarks about possibility of using DODAG root for the coordination of the detection process.
  - ?

Open Floor

AOB

Thank you very much for your attention