Controlling Secure Network Enrollment in RPL Networks

draft-ietf-roll-enrollment-priority-04

Rahul Arvind Jadhav <rahul.ietf@gmail.com>
Pascal Thubert <pthubert@cisco.com>
Huimin She <hushe@cisco.com>
Michael Richardson mcr+ietf@sandelman.ca

post-IETF111 Virtual Interim, August 31 2021

The Story So Far

- Behaviour assumed in RFC9032
- Document Adopted March 2020
- Merged with draft-hushe-roll-dodag-metric after virtual interim meeting January 2021.
- Version -04 posted with merged document
- Reviews and Discussion Summer 2021

RFC9032 – Enhanced Beacon

Protocol Definition

```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       2       |R|P| res |  proxy prio |    rank priority    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| PAN priority  |                                               |
+---------------+                                               +
|                     Join Proxy Interface ID                   |
+                        (present if P=1)                       +
|                                                               |
+               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |                                               |
+-+-+-+-+-+-+-+-+                                               +
|                           network ID                          |
+                  variable length, up to 16 bytes              +
~                                                               ~
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Priority of Join Proxy
(< is better)

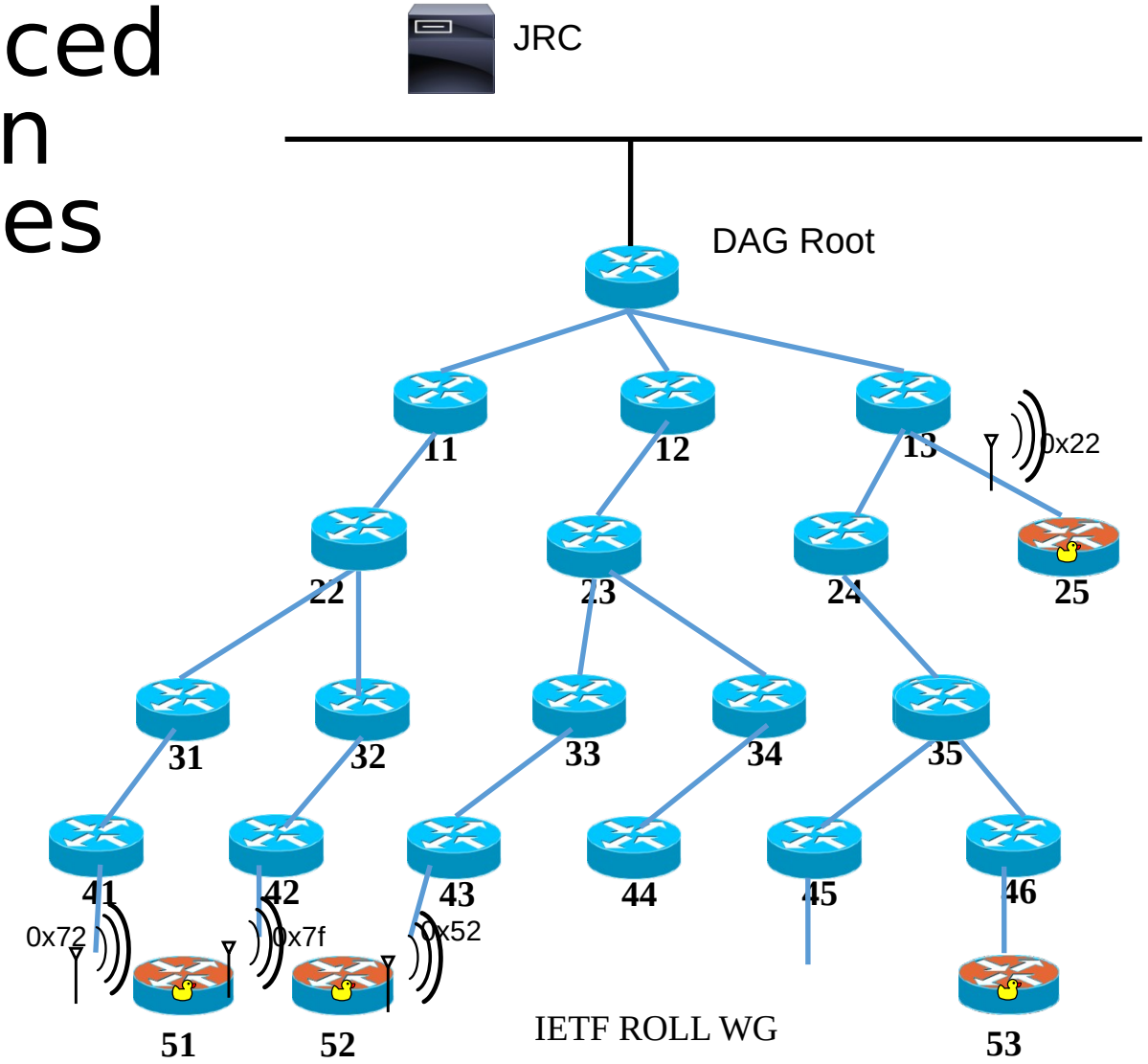
Rank is locally known

Unclear how it is configured, could be added to RFC9031 (CoJP)

Calculated from DODAGID

Included if L2 addr != L3 addr

Enhanced Beacon Samples



Enhanced Beacons

base diagram from PThubert

“The Minimum Enrollment Priority”

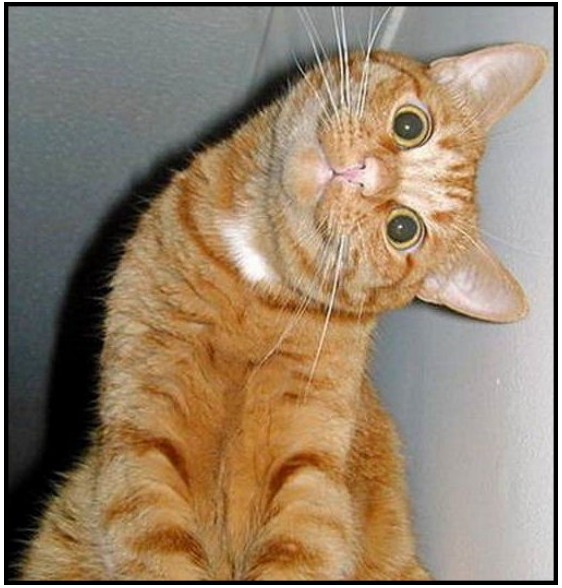
```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type        |Opt Length = 3 |  exp  |     DODAG_Size        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|R| min priority|
+-+-+-+-+-+-+-+-+
```

Issues from Review

- Trickle timer means that DIOs are not sent if there is no topology change.
  - So would changes to min priority be considered a change?
  - The DODAG size field could change quite often, particularly during network formation, how should it be dealt with?
- If updated min priority does not reset Trickle Timer, then this option needs to go into some new flooded control.
  - What are the desired properties of this new control, and what other things should go into it?

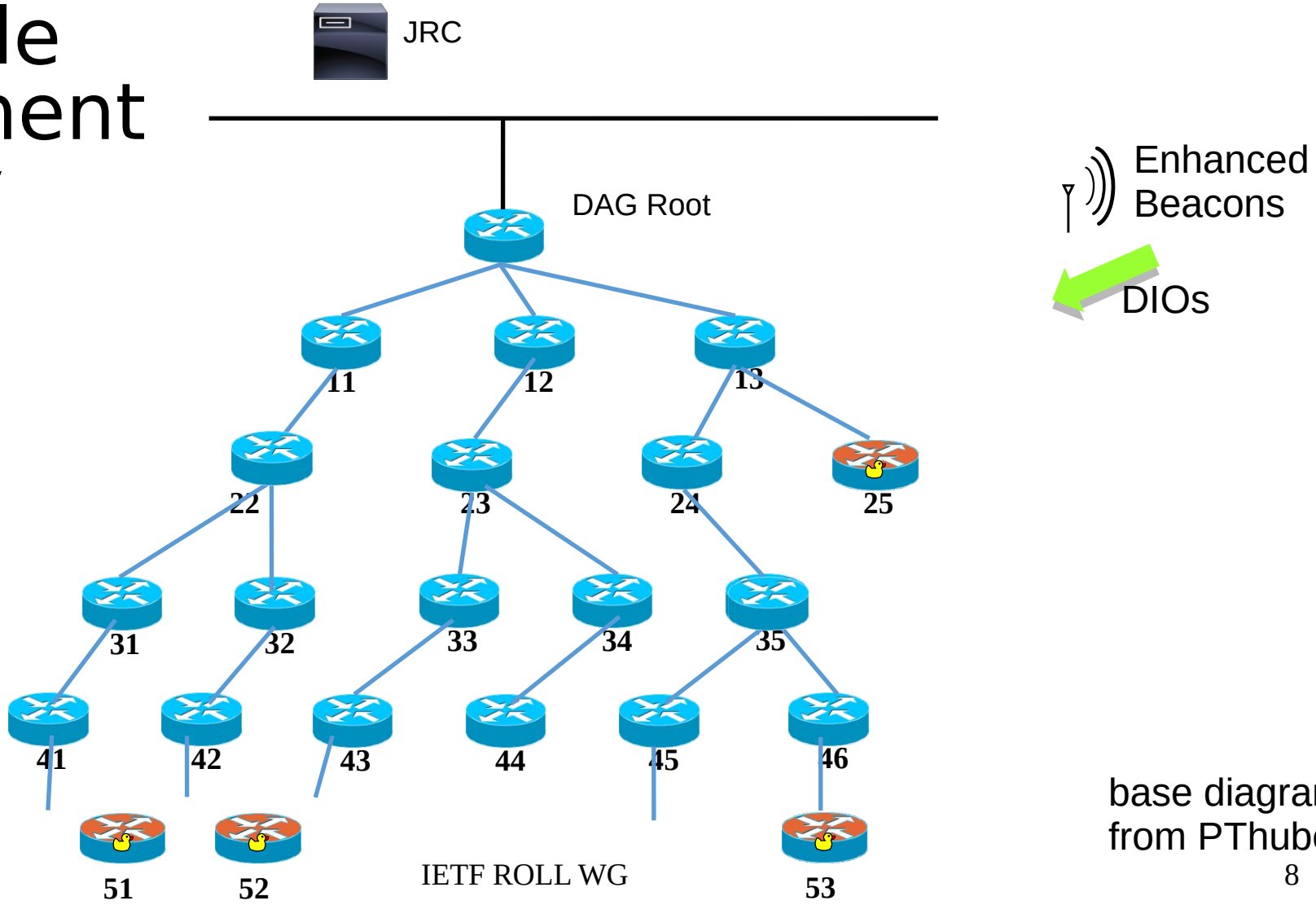
Discussion!

draft-ietf-roll-enrollment-priority-04



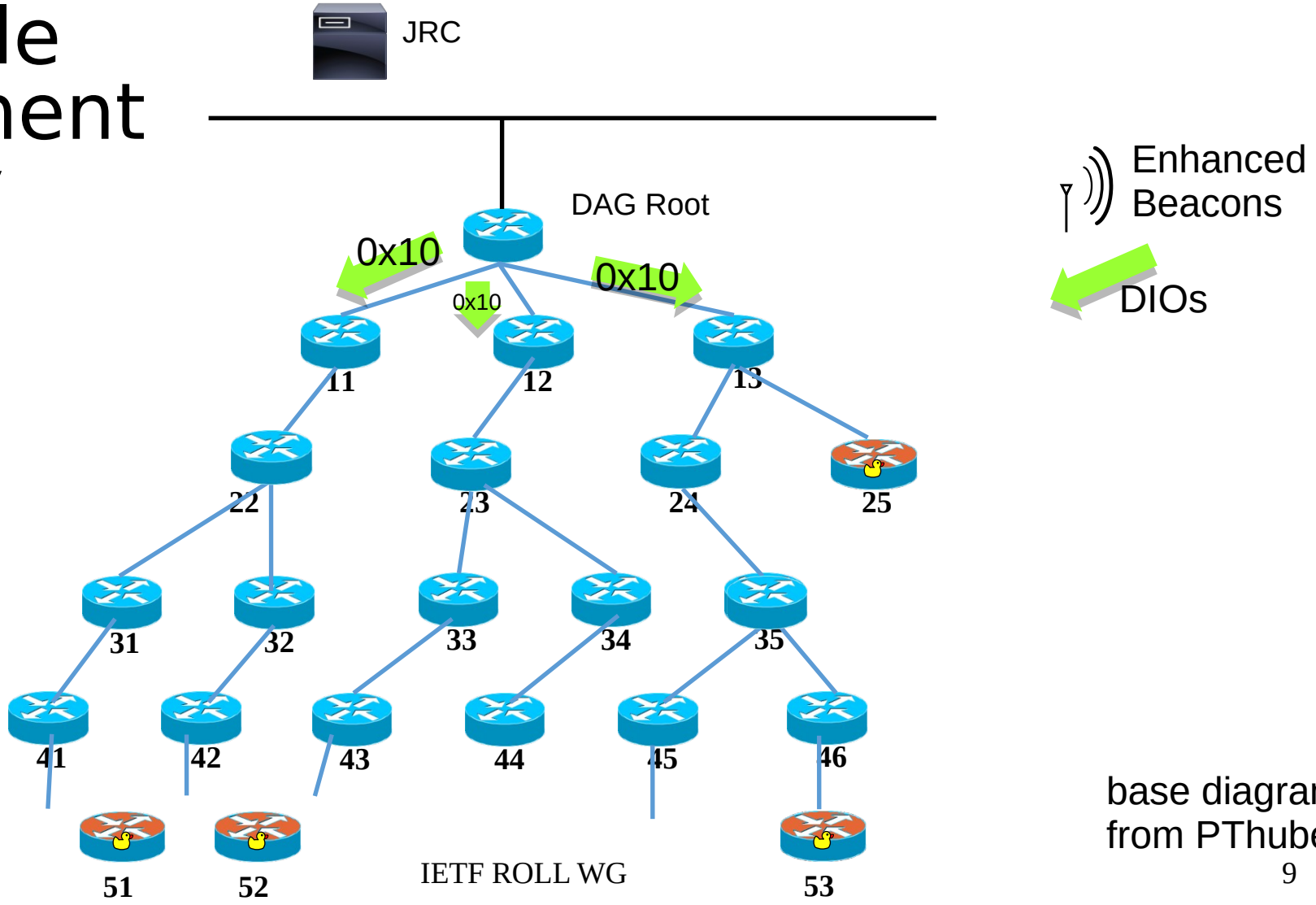
Auxiliary Slides Follow

Example enrollment priority



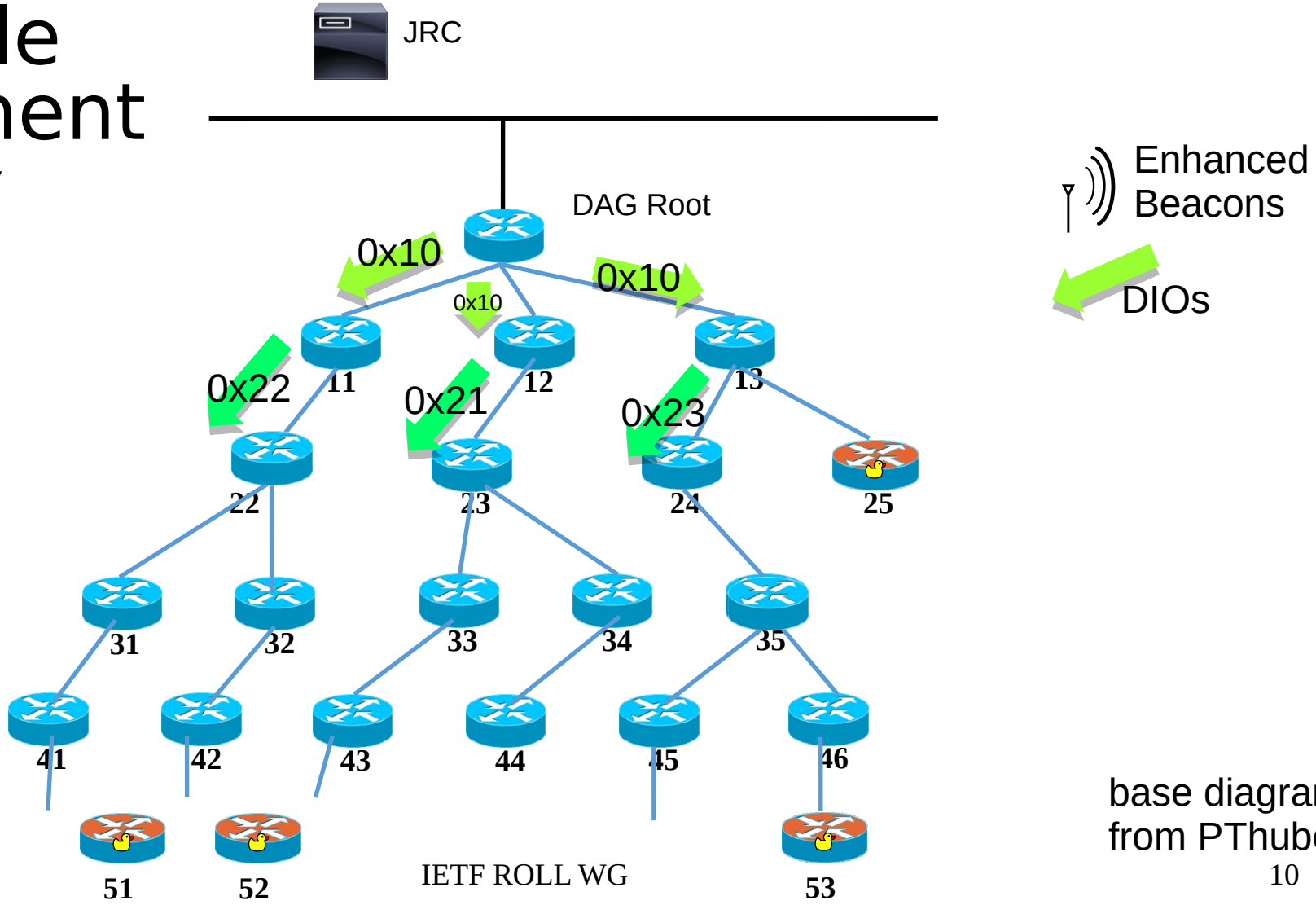
base diagram from PThubert

Example enrollment priority



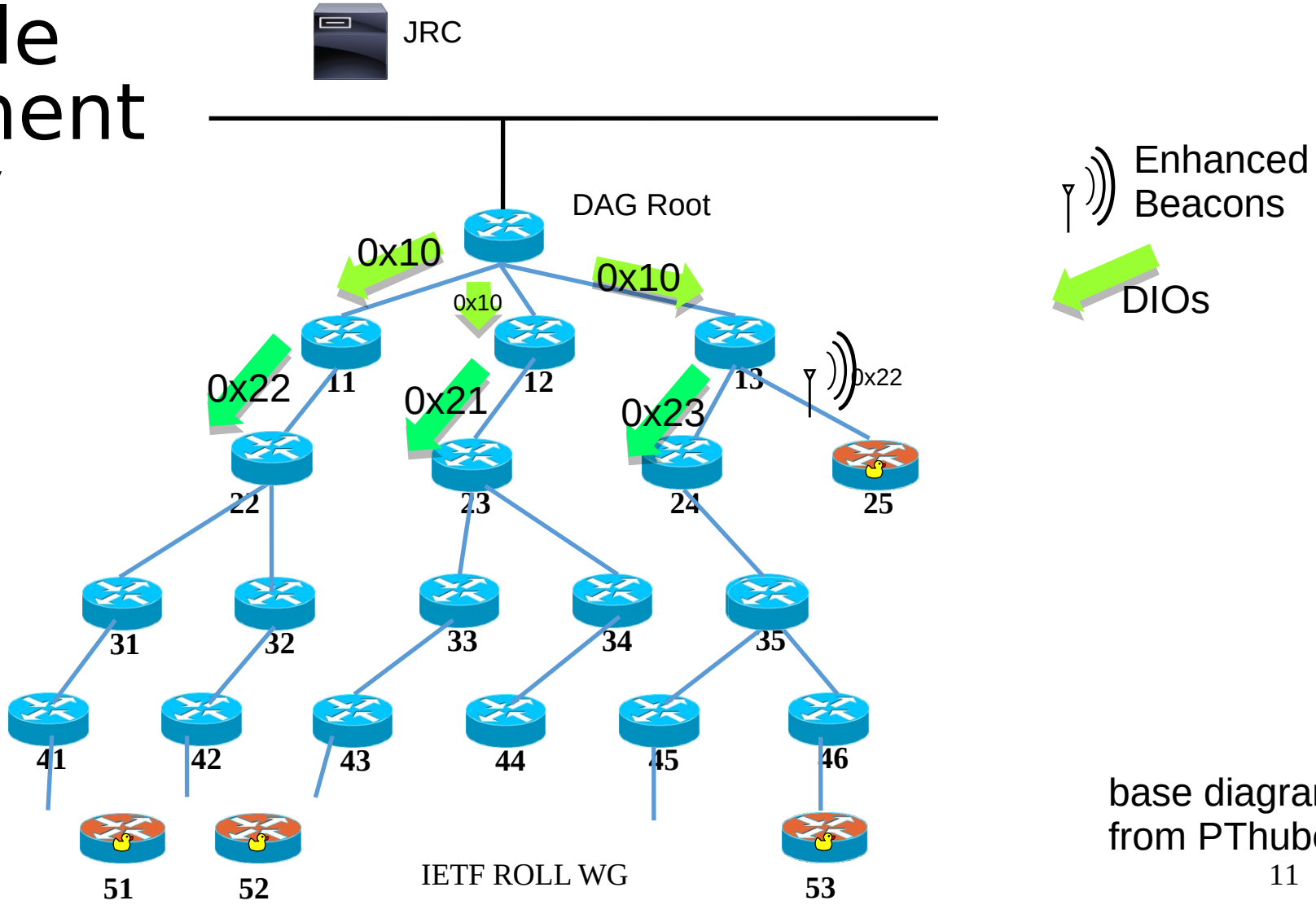
base diagram from PThubert

Example enrollment priority



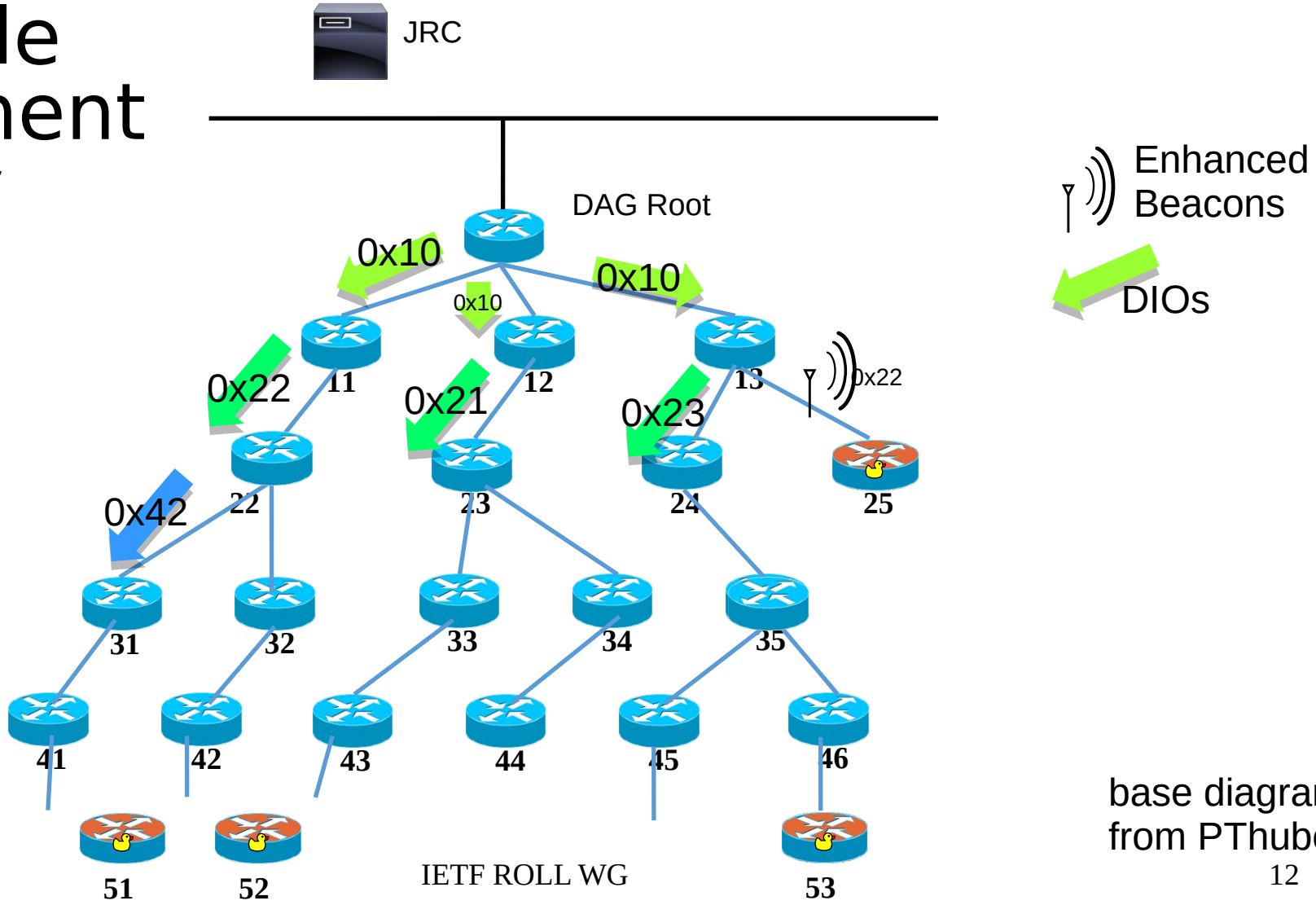
base diagram from PThubert

Example enrollment priority



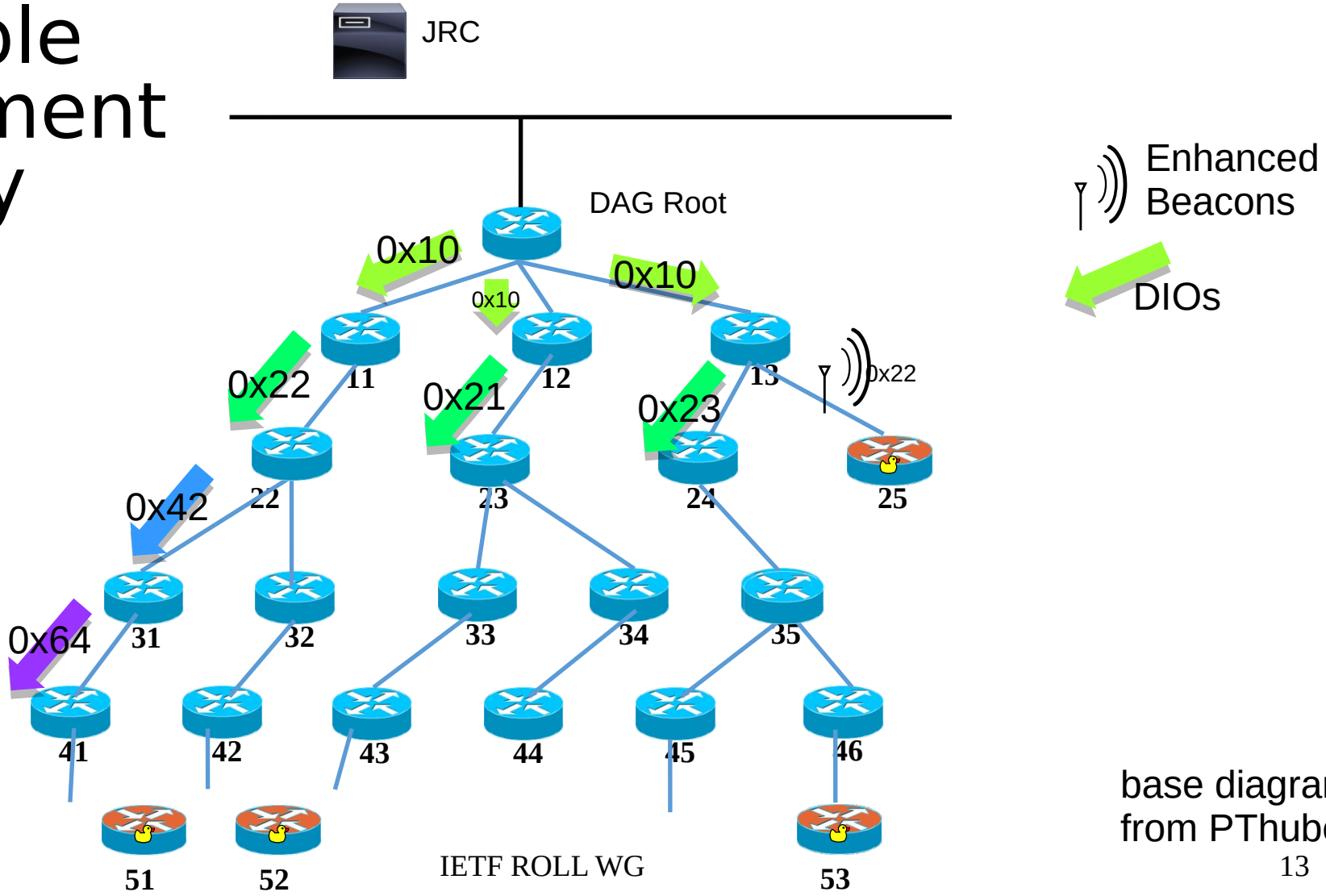
base diagram from PThubert

Example enrollment priority



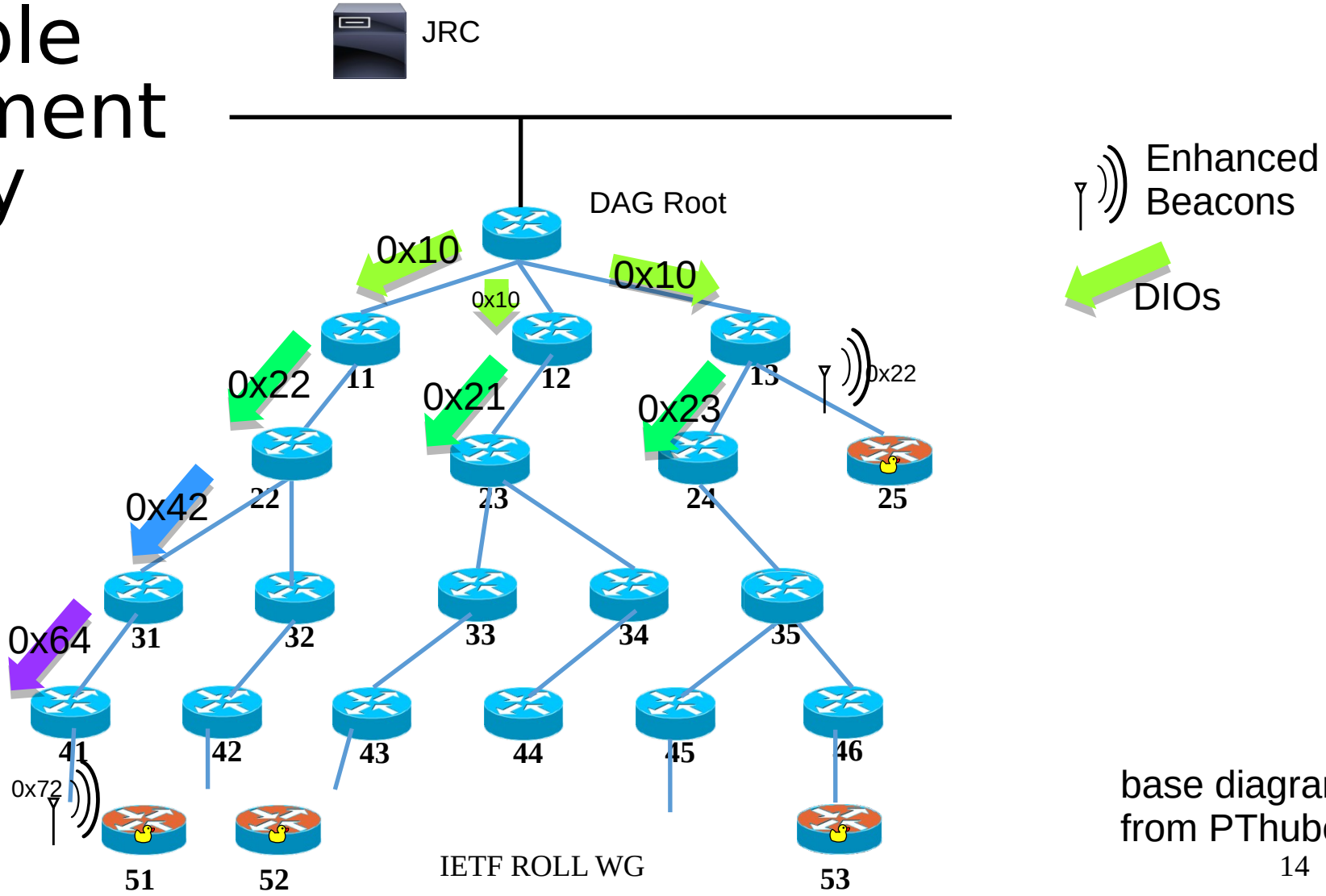
base diagram from PThubert

Example enrollment priority



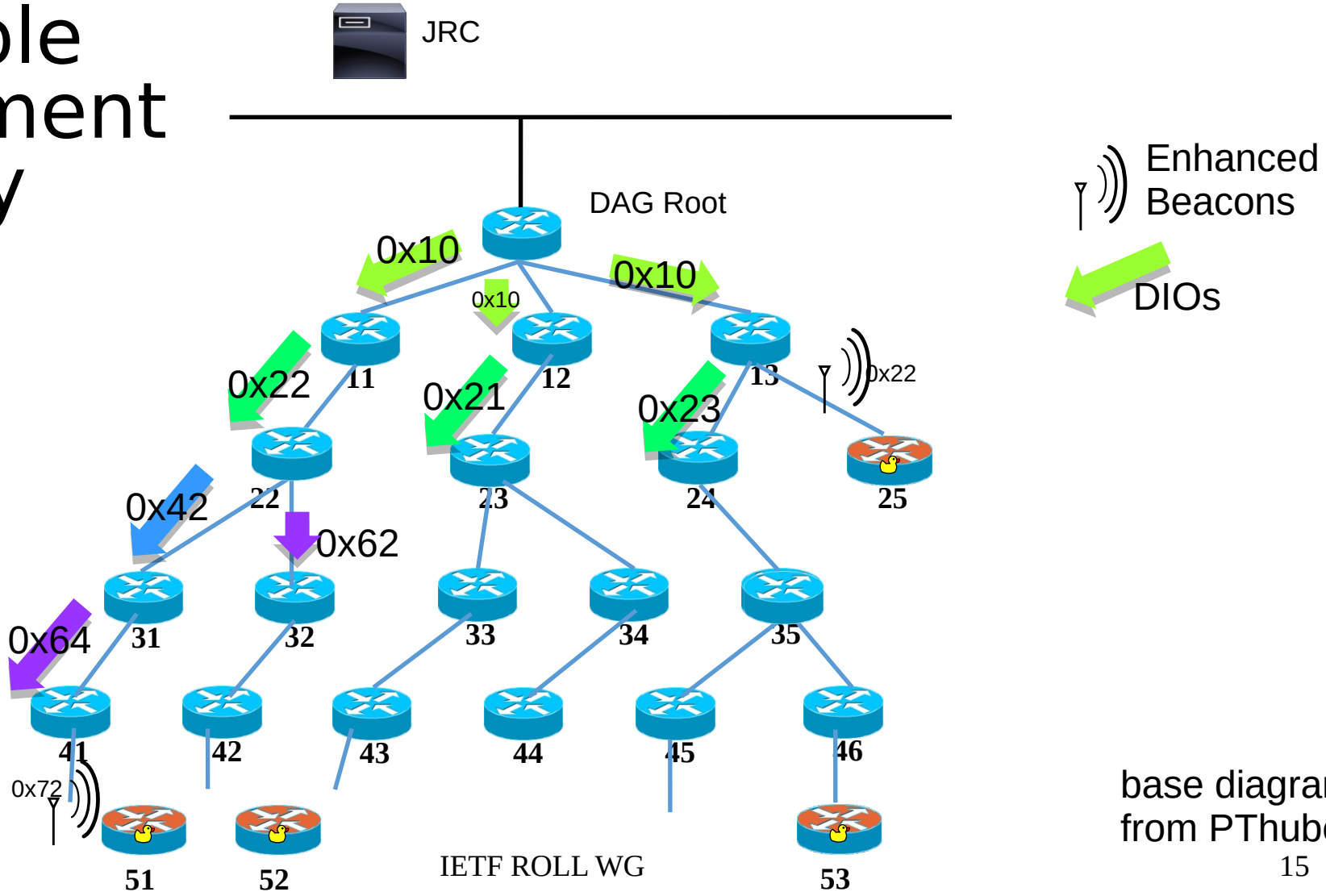
base diagram from PThubert

Example enrollment priority



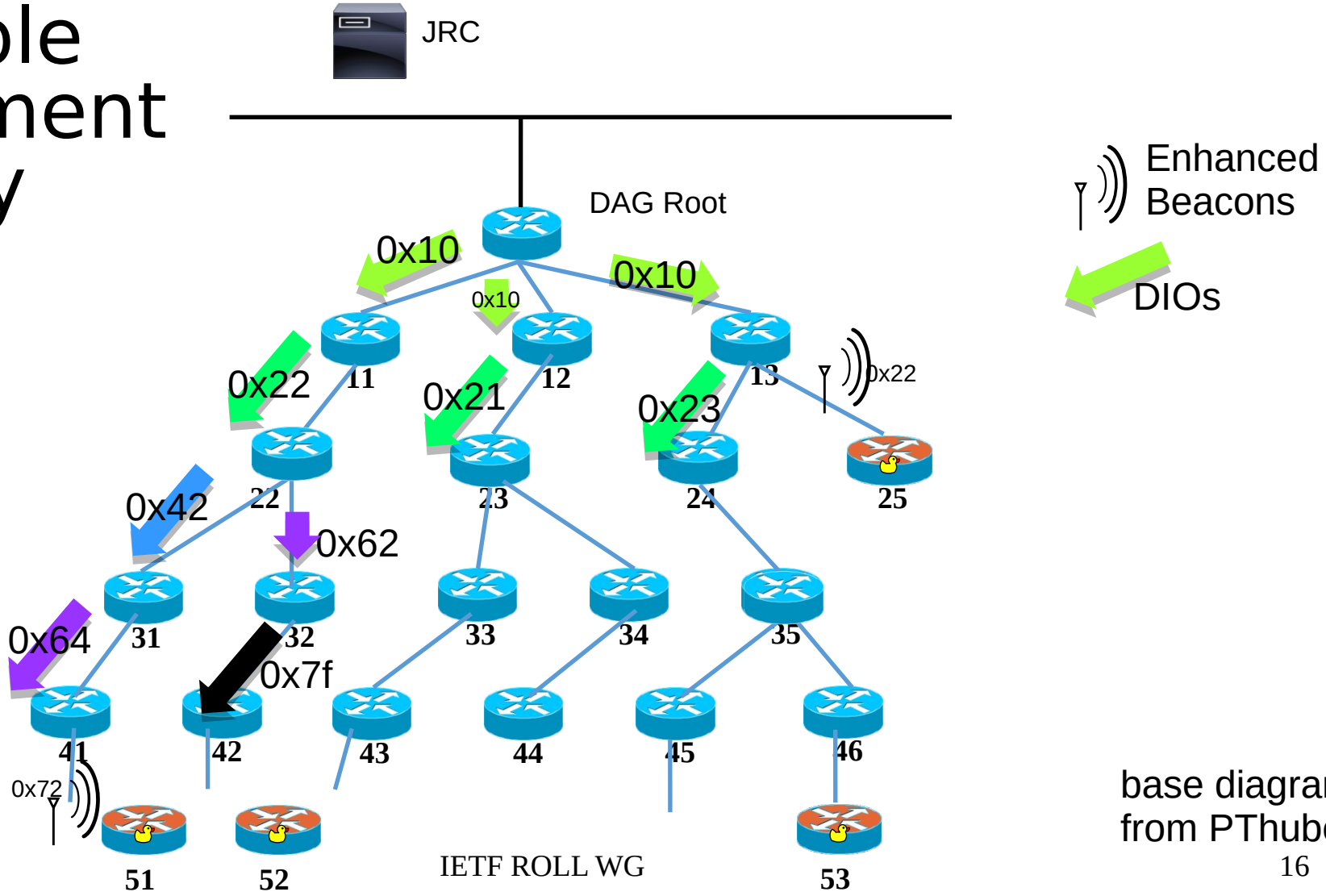
base diagram from PThubert

Example enrollment priority



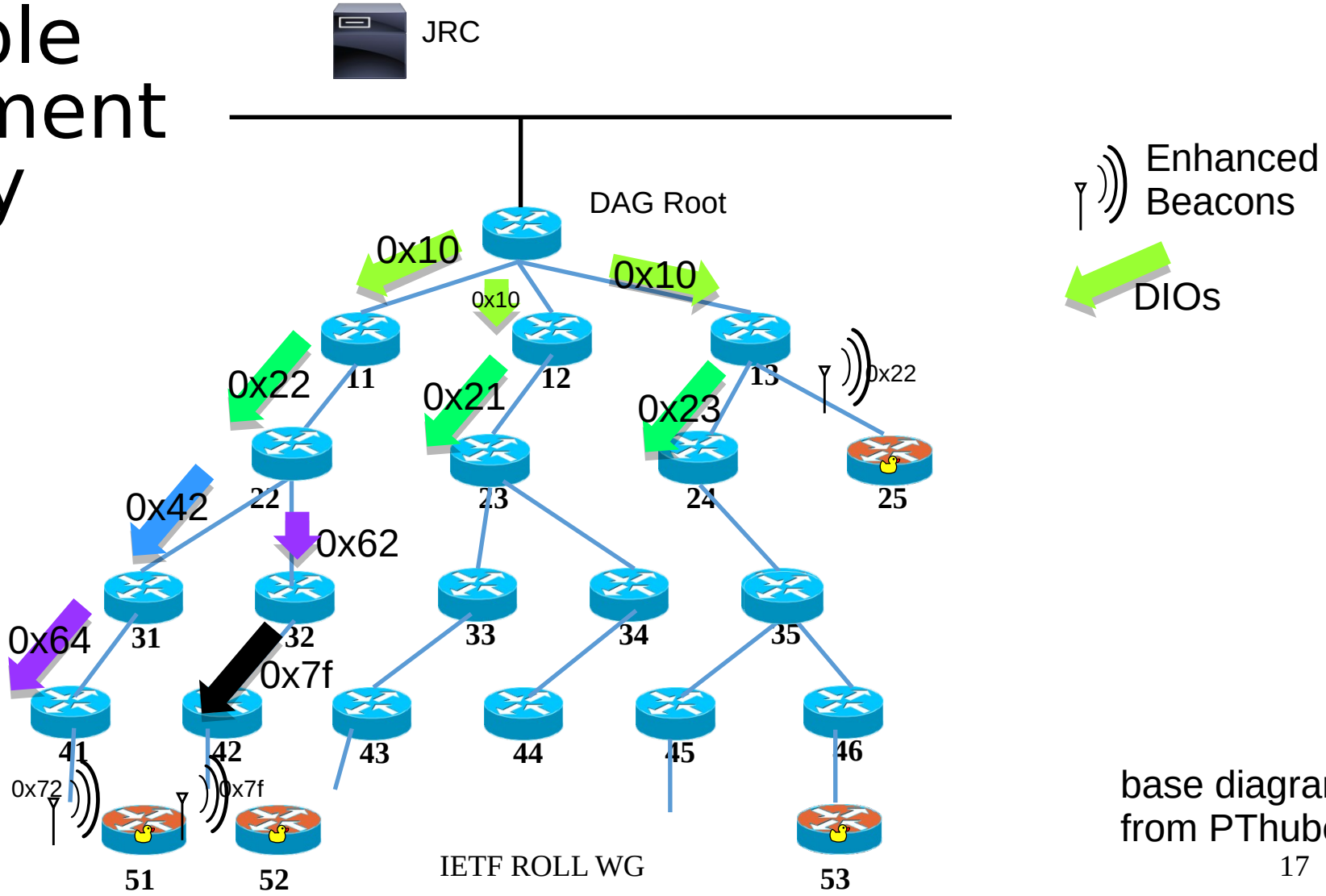
base diagram from PThubert

Example enrollment priority



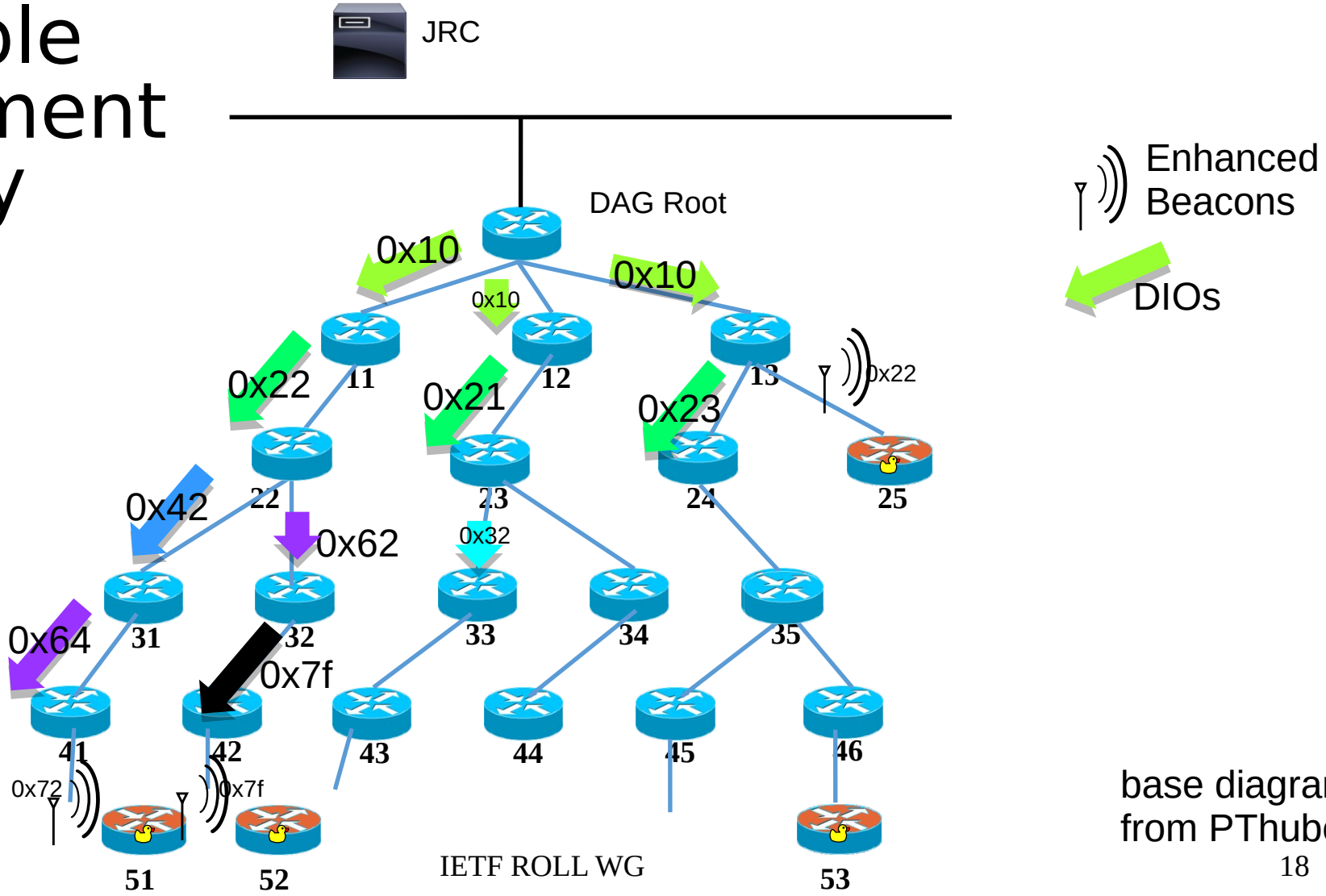
base diagram from PThubert

Example enrollment priority



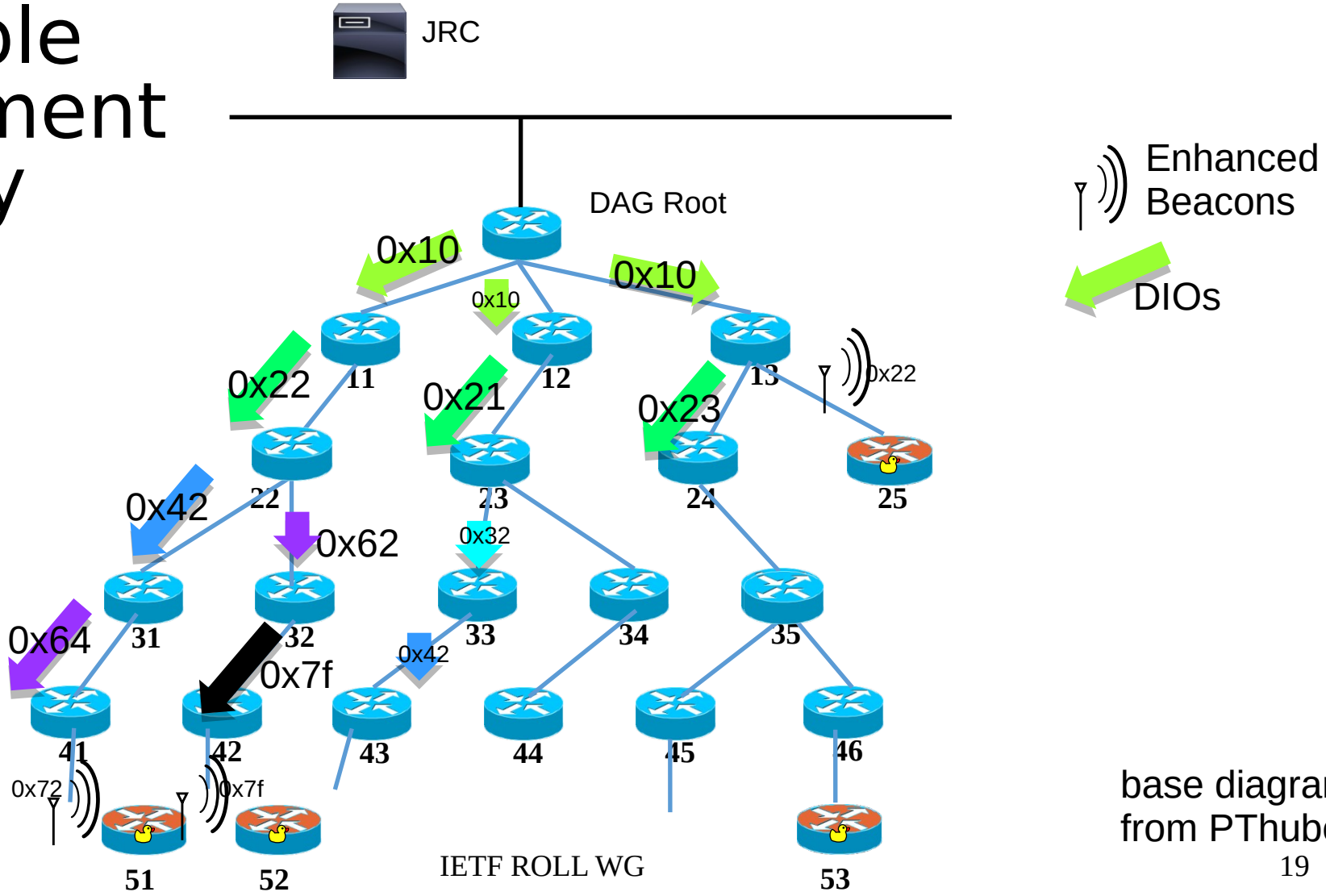
base diagram from PThubert

Example enrollment priority



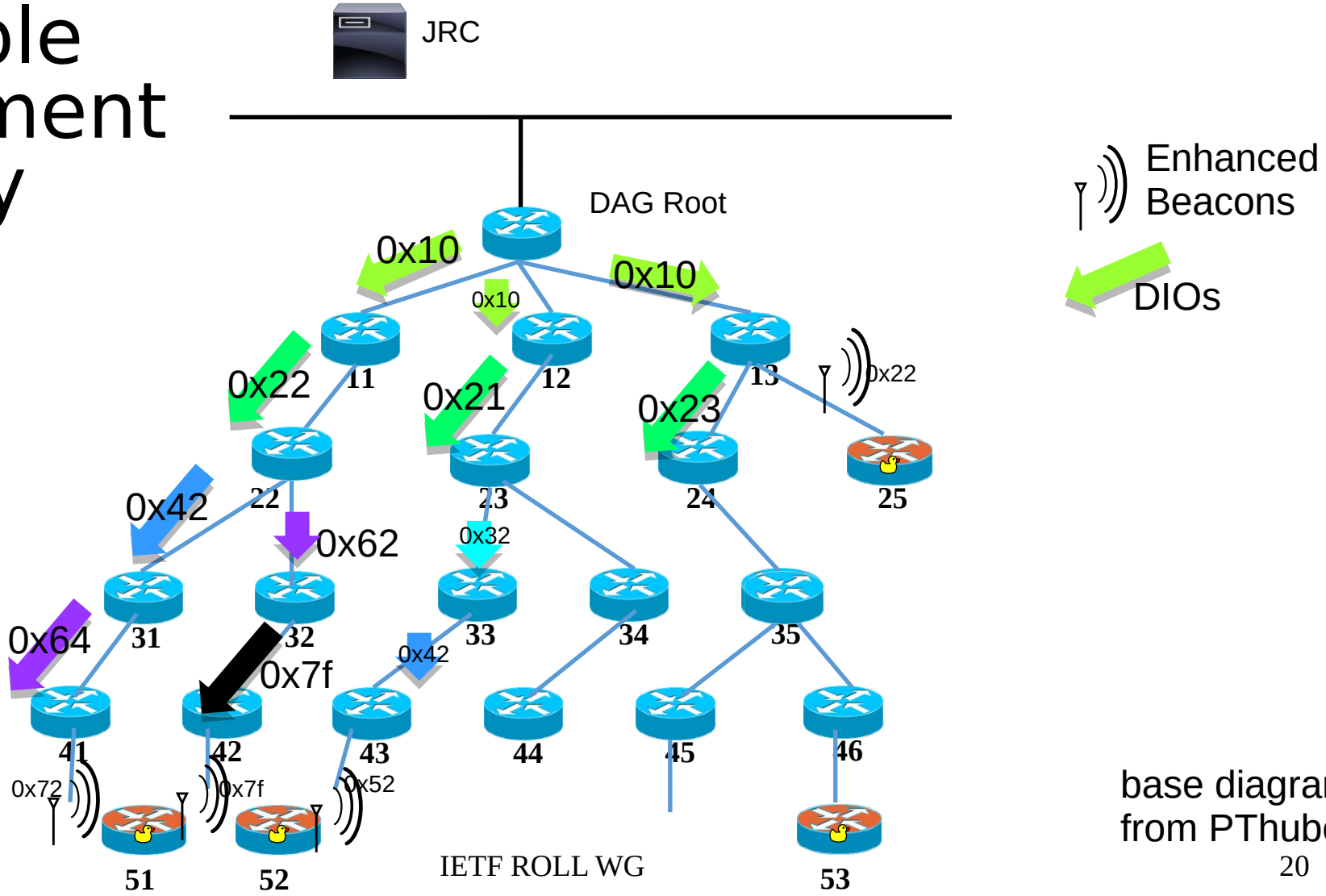
base diagram from PThubert

Example enrollment priority



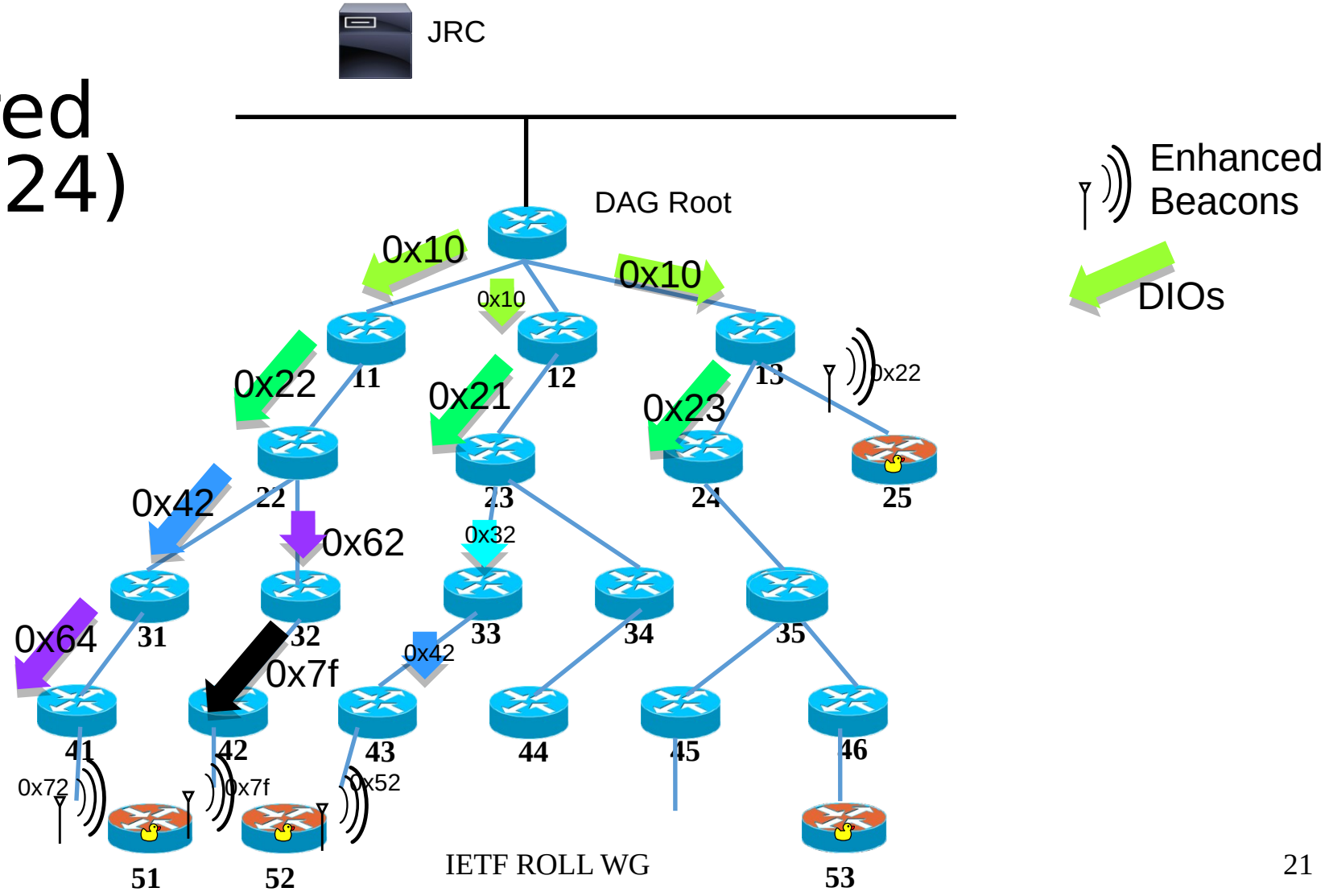
base diagram from PThubert

Example enrollment priority

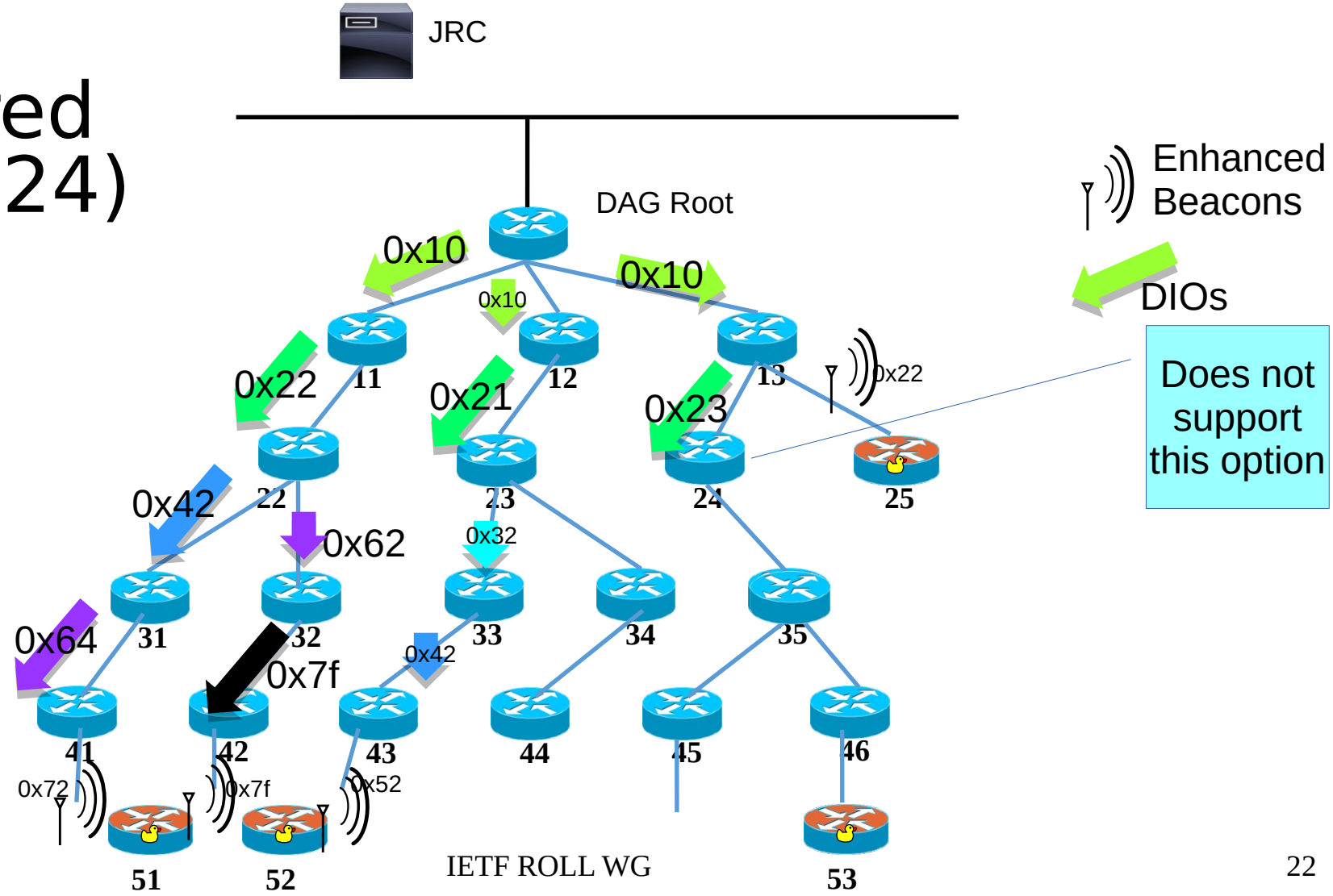


base diagram from PThubert

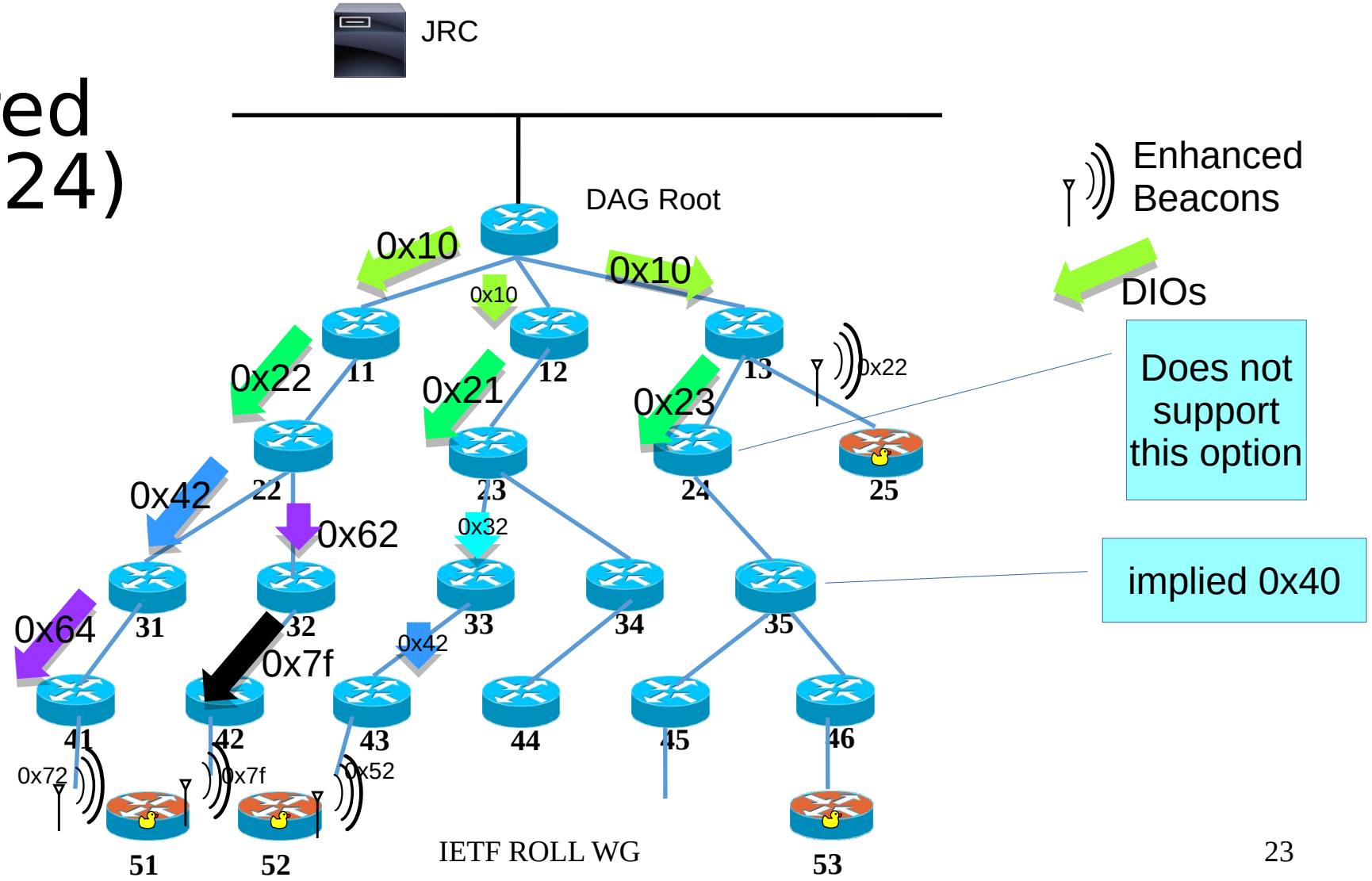
With impaired node (24)



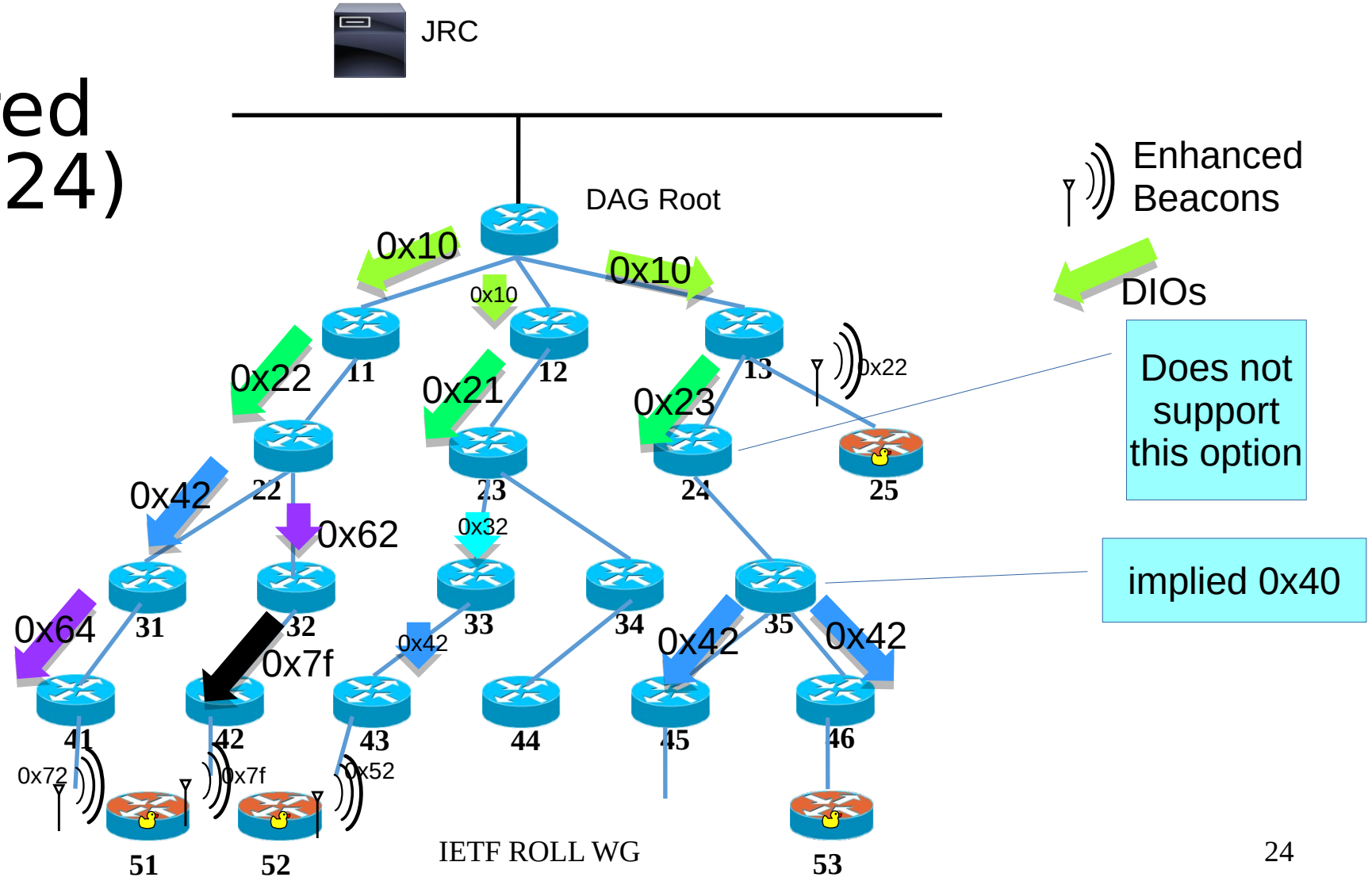
With impaired node (24)



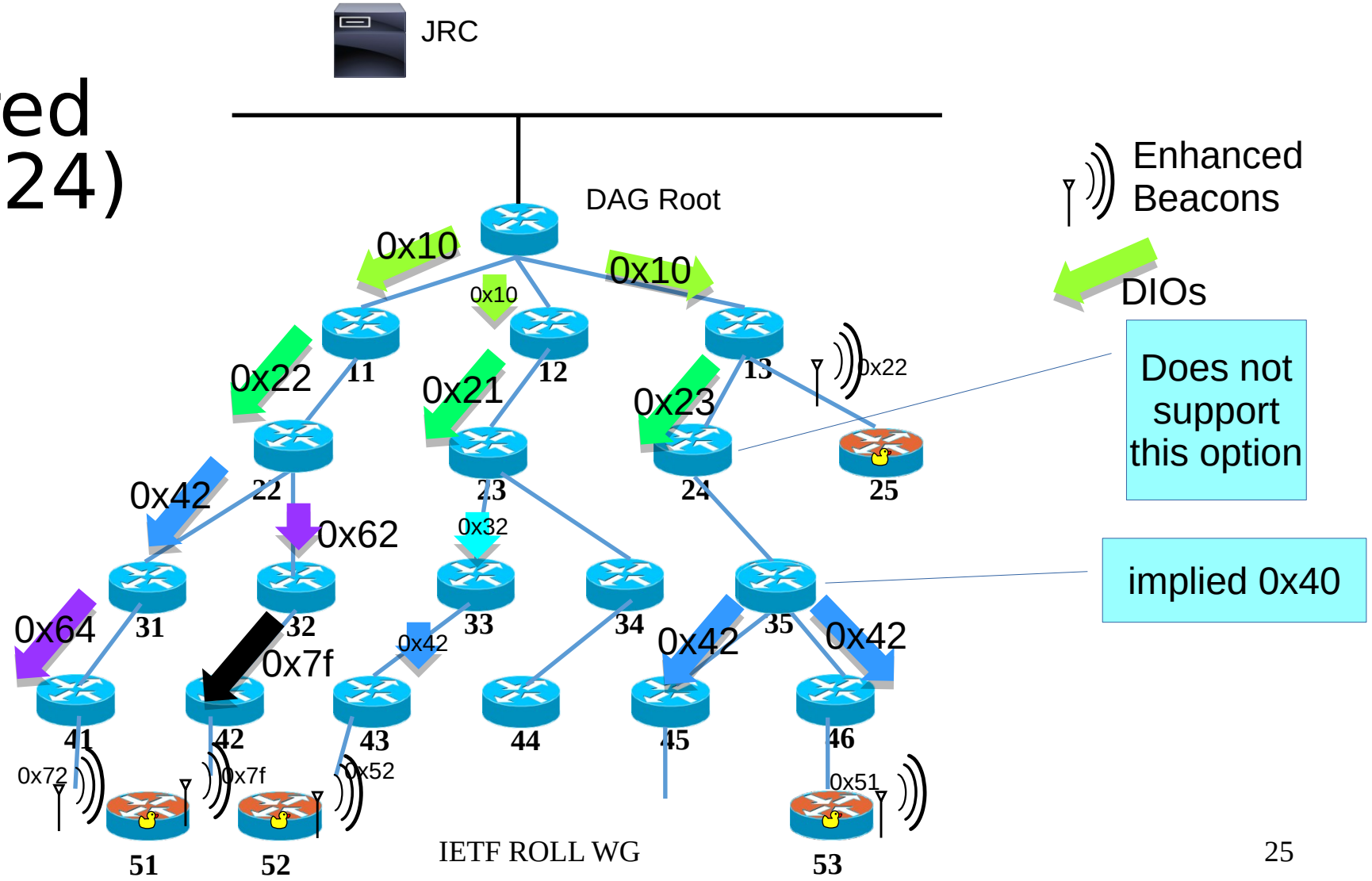
With impaired node (24)



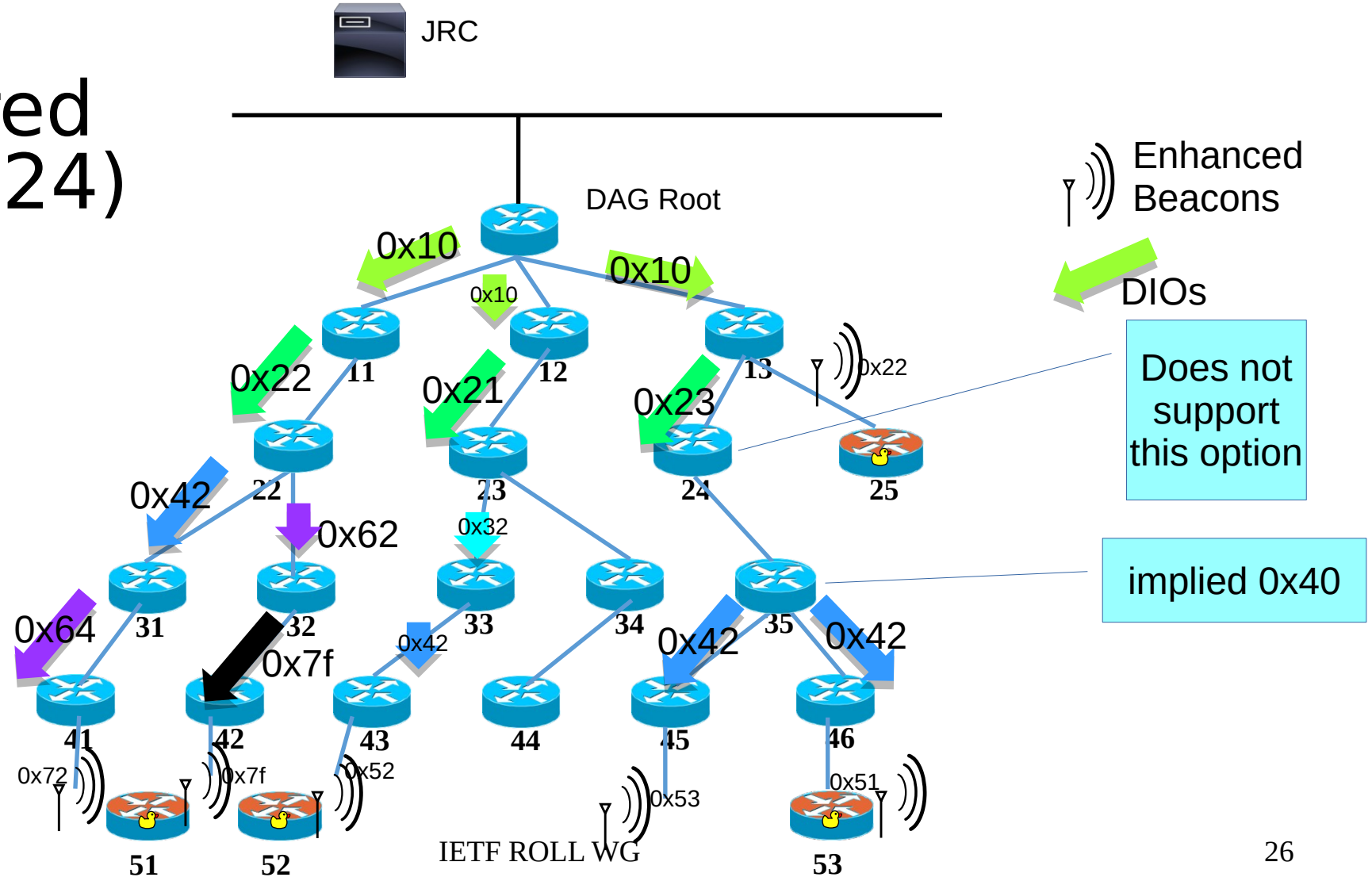
With impaired node (24)



With impaired node (24)



With impaired node (24)



version -04

This document describes an RPL DIO option that can be used to announce a minimum enrollment priority. Each potential _Join Proxy_ would this value as a base on which to add values relating to local conditions. As explained in [I-D.ietf-6tisch-enrollment-enhanced-beacon], higher values decrease the likelyhood of an unenrolled node sending enrollment traffic via this path.

This document describes a RPL DIO option that can be used to announce a minimum enrollment priority. The minimum priority expresses the (lack of) willingness by the RPL DODAG globally to accept new joins. It may derive from multiple constaining factors, e.g., the size of the DODAG, the occupancy of the bandwidth at the Root, the memory capacity at the DODAG Root, or an administrative decision.

Each potential _Join Proxy_ would this value as a base on which to add values relating to local conditions such as its Rank and number of pending joins, which would degrade even further the willingness to take more joins.

When a RPL domain is composed of multiple DODAGs, nodes at the edge of 2 DODAGs may not only join either DODAG but also move from one to the other in order to keep their relative sizes balanced. For this, the approximate knowledge of size of the DODAG is an essential metric. Depending on the network policy, the size of the DODAG may or may not affect the minimum enrollment priority. It would be limiting its value to enforce that one is proportional to the other. This is why the current size of the DODAG is advertised separately in the new option.

As explained in [I-D.ietf-6tisch-enrollment-enhanced-beacon], higher values decrease the likelyhood of an unenrolled node sending enrollment traffic via this path.