Efficient IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks

draft-chakrabarti-nordmark-6man-efficient-nd-02

Samita Chakrabarti
(Samita.chakrabarti@ericsson.com)
Erik Nordmark
(nordmark@cisco.com)
Pascal Thubert
(pthubert@cisco.com)
Margaret Wasserman
(mrw@lilacgrade.org)

Background

- The Idea was first presented at IETF 82(6man, intarea):

  draft-chakrabarti-nordmark-energy-aware-nd-xx

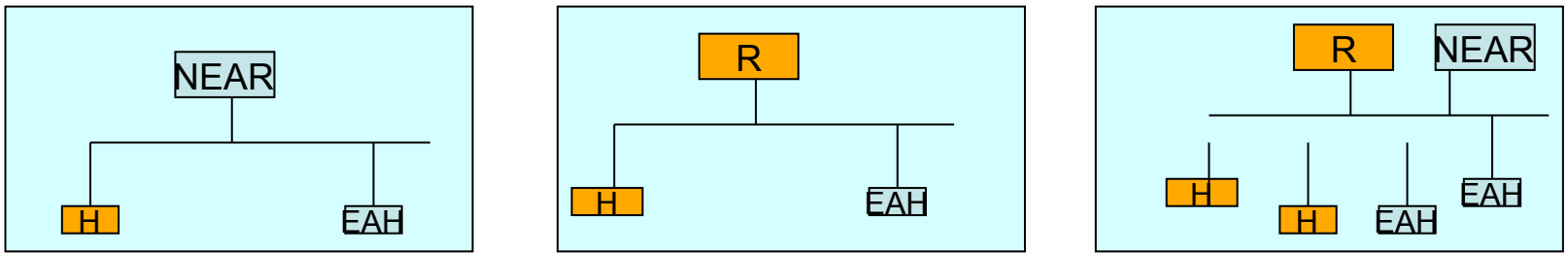
- Next presentation in IETF 85 with focus on general efficiency in IPv6 networks and its interaction with protocols – DNA, DHCPv6, ND Proxy, MLD Snooping

  draft-chakrabarti-nordmark-efficient-nd-01

- The solution handles classic ND and enhanced ND operations

What is Efficient-ND?

- Leverages 6lowpan-nd [RFC 6775] for general IPv6 links
  - No periodic multicast RA
  - Replaces DAD with Address Registration Option [ARO]
  - No multicast NS messages
  - Host-driven refresh of RA information – unicast RS to refresh
- Adds support for mixed-mode links
  - Combining RFC 4861 and efficiency-aware nodes on same link
  - Defines a new E-bit in the RA so hosts know the efficiency-aware routers
- Allows for sleeping hosts
  - ARO is used to check for duplicates at the router
- ND host scan attack removed/reduced
  - As more hosts use ARO the rate limit for sending multicast NS can be reduced to zero when all hosts on link use ARO
- Interactions with DHCPv6, DNA, MLD-snooping etc.
  - Clarifications about any change in behavior of the above protocols



In this edition (-02)

Existing:

- Basic Optimization of reduced multicast ND messages and address registration

New Addition

- Handling out-of-order registration in a link with high delay variation
  - Addresses inter-backbone router movement
  - Supports RPL Routing protocol with TID
- Partial registration or multi-registration in a wireless link with default routers by a mobile host

Removal

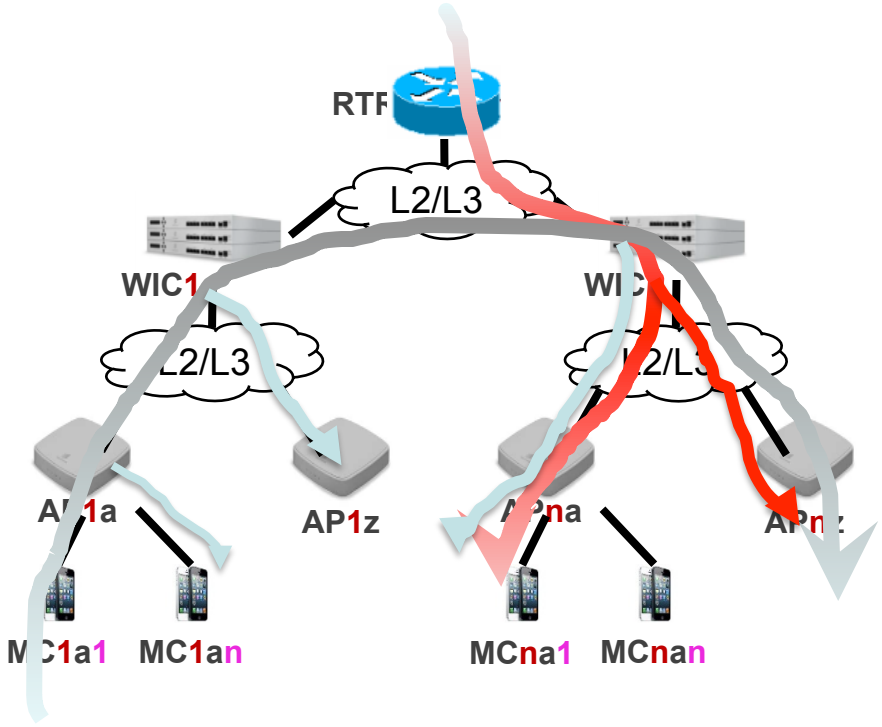
- Use case analysis Details

Avoiding multicast/broadcast issues in WIFI networks

A motivation to solve the following problem

The WiFi bridge network amplifies the downstream broadcast and multicast traffic at both the AP and controller. There are two sources of downstream traffic.

- Core network traffic going toward controllers, and controllers replicate this broadcast/multicast traffic to all of it physical (Eth: LAN & WAN) and virtual (CAPWAP) interfaces
- Mobile client traffic going to the Core network; and controllers replicate this (IPv4-ARP, IPv6-ND) traffic to all of it physical (Eth: LAN & WAN) and virtual (CAPWAP) interfaces

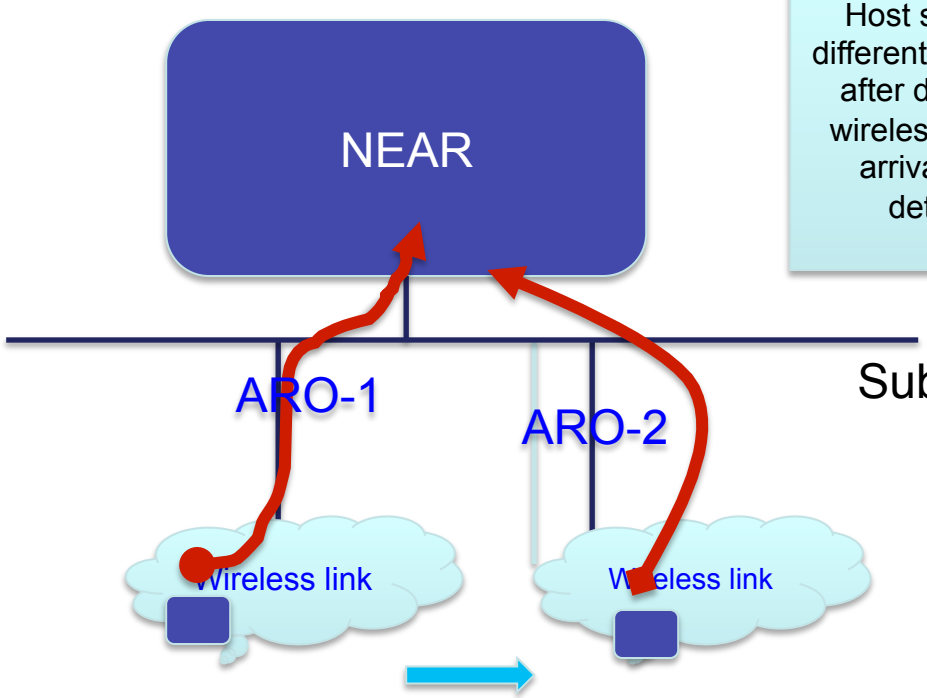


Solution:
Optimization on mcast, DAD, periodic RA + Introducing ARO

Implementations are coming up with vendor specific solutions to avoid the amplification

Out-of-Order Registration Handling

- ARO contains TID

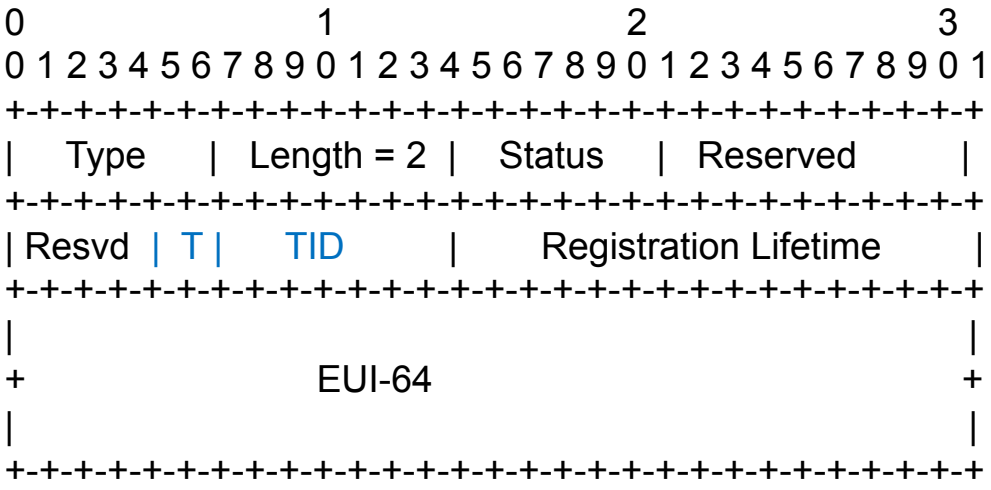


Host sends ARO-1 and then moves to a different wireless link and then sends ARO-2 after detecting L2 –link move. But due to wireless network delay ARO-2 and ARO-1 arrival order is revered. TID is used to determine newest registration link

TID comparison also helps movement in Backbone routers, RPL (Pascal)

Address Registration Option (updated)

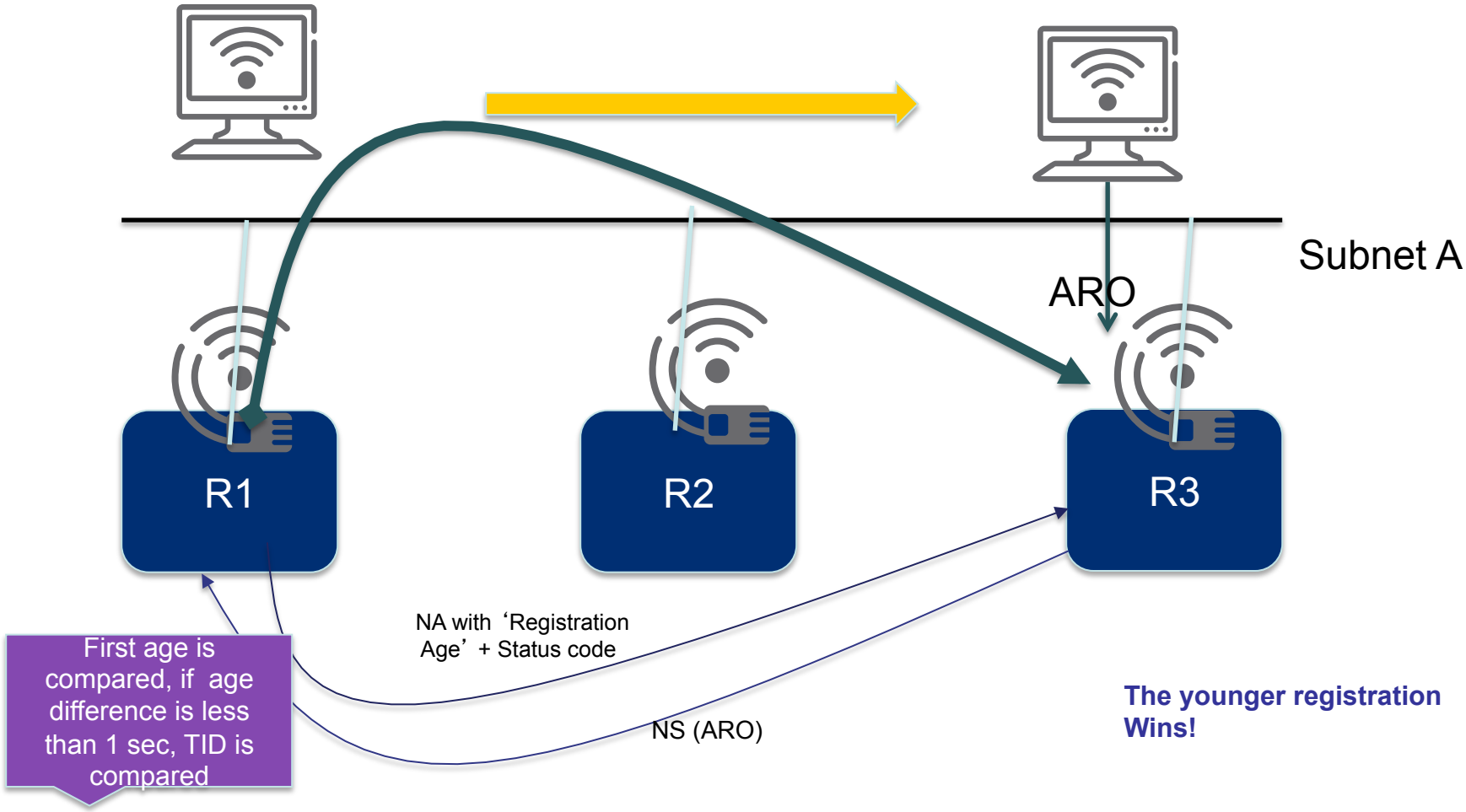
- Address Registration Option (ARO) is sent by the efficiency-aware hosts in a unicast NS message
- Optionally ARO may be sent by the NEAR to another NEAR in order to resolve ownership of registration
- TID field may be used by the NEAR routers to detect duplicate registration and as well as local mobility



ARO with NS from Node.

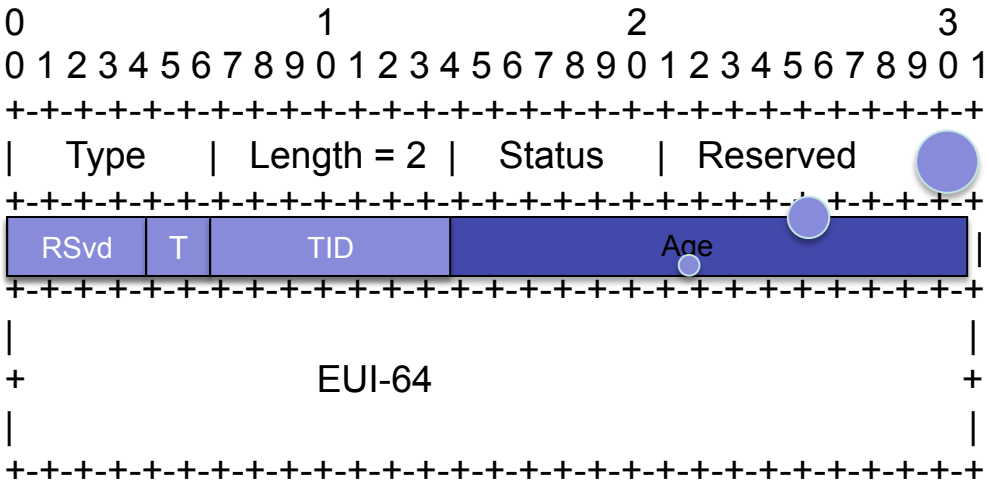
Partial registration and Local Mobility Solution

- The Wireless node moves and registers with the closest router for efficiency ; The routers negotiates among themselves who should win the registration and then inject /delete routes to the network accordingly
- The ‘Partial registration solution’ is not mandatory but recommended



Address Registration Option with NA
(when used between NEAR routers)

- Address Registration Option (ARO) is included by the efficiency-aware routers in a unicast NA message
- The ‘Registration Lifetime’ field is used by the NEAR routers (optionally) to resolve the conflict resolution in order to update the ownership of the registration of the node



Alternative Idea: use an option to ARO for ‘age’

ARO with NS from Node.

Open Issues

- Current ‘age’ information is only exchanged by NEAR but it uses the same ‘Registration lifetime field’ in NA with a status code =3 to indicate that the field contains age ownership response.

- Should we avoid the overloading of field by introducing options to ARO?

Next Step

- Requesting the working group to move this document as the wg item
- Comments are welcome

Thanks!

Backup Slides

NEAR and EAH in Mixed-Mode

NEAR

- Sends periodic RAs for legacy hosts
- Supports ARO for EAH
- Advertises E-bit in RA
- Manages both Registered NCE entries and Legacy entries
- SHOULD have configuration knobs for Mixed vs. Efficiency-aware-only mode
- Recommended default mode for NEAR is Mixed-Mode
- NEAR MUST NOT set ‘L’ bit in RA

EAH

- First sends Multicast RS to the link to detect presence of NEAR if it did not hear a RA with E-bit upon joining the network already
- If it hears from both NEAR and legacy IPv6 Router, the NEAR(s) gets preference as a default router(s)
- Registers with more than one NEAR (if multiple are available)
- Efficiency-aware hosts SHOULD de-register before it moves away or switches to legacy mode

Mixed-mode

- Legacy host multicasts DAD probe
  - In mixed mode, NEAR proxies based on registered NCEs
- Legacy host sends data packet to any router since L=0
  - Legacy router would multicast NS
  - NEAR would proxy with an NA based on registered NCEs
  - [Alternative is to require that a mixed link has only NEAR routers]
- EAH uses ARO for DAD
  - In mixed mode, NEAR should multicast DAD probe before ack'ing ARO

Interaction

- Detecting Network Attachment (DNA)
  - Orthogonal
  - DNA sends a unicast NS to previously know router(s)
  - That can now include an ARO
  - DNA also sends a multicast RS (in case moved to new link)
  - Same as a regular RS/RA on power-on
- DHCPv6
  - ARO is used for link-local address
  - DHCPv6 client SHOULD check DAD for assigned address. If ARO is available use that instead of multicast DAD probe
- Secure ND
  - RFC 37971 recommends allowing un-secured DAD on first try
  - Allows for NEAR to proxy DAD respose
- MLD snooping
  - No use of solicited-node multicasts means less MLD snooping state

NCE Management

- Two Types of NCE
  - Legacy (RFC 4861 NCE)
  - Registered (in mixed-mode and efficiency-aware only mode)
- NCE types are orthogonal to NCE states

- All NCE are started with Legacy NCE
  - Turns into ‘Registered’ NCE upon successful processing of ARO
- Registered NCE are NOT garbage-collectable
  - Registered NCE has its own life-time
  - Registered NCE are renewed by the EAH via Registration refresh before it expired

- In efficiency-aware only mode a TENTATIVE legacy NCE is created for a short time and deleted if the entry does not get registered

- Registration lifetime and EUI-64 are recorded for Registered NCE

- Only **one** type of NCE can exist in Neighbor Cache at a time

Handling ND-DOS Attacks

- Only in efficiency-Aware mode
- Tentative NCE entries are discarded if registration fails
- Duplicate entries must be checked before creating a valid NCE entry by checking EUI-64, MAC-address and IP-address
- All RS requests MUST contain SLLA option and avoids Neighbor Solicitation for the requestor's address resolution

Handling Sleepy Nodes

- Sleepy nodes must support efficiency-aware mode only behavior
- No Multicast periodic RA
- No Address resolution Required
- Address Registration ensures duplicate checks
- Uses Default-router for packet forwarding
- Sleep and Registration interval should be synchronized for maximum energy savings