# IPv6 over Low power WPAN WG (6lowpan)

Chairs:

**Geoff Mulligan <geoff@mulligan.com>**

**Carsten Bormann <cabo@tzi.org>**

Mailing List:

**6lowpan@ietf.org**

Jabber:

**6lowpan@jabber.ietf.org**

- **We assume people have read the drafts**
- **Meetings serve to advance difficult issues by making good use of face-to-face communications**
- **Be aware of the IPR principles, according to RFC 3979 and its updates**

✓Blue sheets
✓Scribe(s)

# Milestones (from WG charter page)

**Document submissions to IESG:**

- **Aug 2008 x 2 Improved Header Compression (PS)**
- **Aug 2008 // 6 Security Analysis (Info)**
- **Sep 2008 // 3 Architecture (Info)**
- **Sep 2008 x 4 Routing Requirements (Info)**
- **Nov 2008 x 1 Bootstrapping and ND Optimizns (PS)**
- **Dec 2008 x 5 Use Cases (Info)**

**Also: running documents for implementers, interop**

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |

# 6LoWPAN Security Analysis

**Soohong Daniel Park (Samsung)**
**Ki-Hyung Kim (Ajou univ.)**
**W. Haddad (Ericsson) (Ed.)**
**Samita Chakrabarti (IP infusion)**
**Julien Laganier (Qualcomm)**

# Draft Status

- **Analysis and study on 6lowpan security (Info track)**
  - **Don’t spell out any solutions for 6lowpan security**

- **03 version in July 2009**
  - **Whole document is reviewed and updated by Wasim Haddad (Ericsson).**

# Draft Skeleton

- Overview
- Security Challenges
- Security Requirements
- Security Threats
- Assumptions
- 6lowpan security analysis
  - IEEE 802.15.4 Security analysis
  - IP Security analysis
- Key Management in 6lowpan
  - Existing Key management methods
  - Issues with Key management in 6lowpan
- Security consideration in bootstrapping a 6lowpan node

# Basic Assumption

- **The [RFC 4919] describes two security concerns as follows;**
  - **In Section 4.6 Security: IEEE 802.15.4 mandates link-layer security based on AES, but it omits any details about topics like bootstrapping, key management, and security at higher layers. Of course, a complete security solution for LoWPAN devices must consider application needs very carefully.**
  - **In Section 5 Goals: Security Considerations: Security threats at different layers must be clearly understood and documented. Bootstrapping of devices into a secure network could also be considered given the location, limited display, high density, and ad-hoc deployment of devices.**

## ➔ This draft is feeding out the above requirements

- **In addition, existing IP security technologies will be simplified to be implemented on the 6lowpan small devices. 6lowpan security architecture will shed off lots of fat from IP security technologies whenever available.**
- **IEEE 802.15.4 AES (Advanced Encryption Standard) will be used for 6lowpan security architecture in conjunction with IP security whenever available.**

# Moving Forward

- **Significantly improved from 02**
  - **Hopefully ready for WG adoption, Should we move forward?**
- **Further input and work from SECURITY guys**

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |

# 6LoWPAN MIB

IETF-76 Hiroshima

(draft-daniel-6lowpan-mib-01)

Kim Ki Hyung, Hamid Mukhtar, S.S Joo, S Yoo, S. Daniel Park

# 6LoWPAN MIB

- MIB module for 6LoWPAN node
  - 6LoWPAN Generic parameters
  - Route Over parameters
  - 6LoWPAN Mesh parameters (optional)
  - 6LoWPAN statistics
  - Relationship and compliance with other MIBs
- Define MIB module for ER (?)

# Generic parameters for the 6LoWPAN node

- 6lowpanDeviceRole
- 6lowpanDeviceCapabilities
- 6lowpanRoutingProtocol
  - RPL, DADR, DV, Dymo-Low, Load, etc
- 6LowpanRoutingTable (?)

# Other parameters

- Route-Over parameters
  - ND parameters (?)
    - Edge Router List
    - TBD
- 6LoWPAN Mesh parameters (for mesh-under only)
  - 6LowpanNeighborTable
  - 6lowpanUseHierarchicalRouting
  - 6lowpanBroadcastSequenceNumber
  - 6lowpanAckTimeout

# 6LoWPAN statistics

- Number of fragmentation errors
- Number of reassembly errors
- TBD

# Relationship with other MIBs

- Relationship with other MIBs
  - IP-MIB
    - IPv6 specific variables
  - Interfaces MIB (IF-MIB) module
  - TBD
- Compliance for other related MIBs
  - ENTITY-SENSOR MIB
  - TBD

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |

# SNMP Optimizations for 6LoWPAN

IETF-76 Hiroshima

(draft-hamid-6lowpan-snmp-optimizations-02)

Hamid Mukhtar, Juergen Schoenwaelder, Seong-Soon Joo, Kim Ki-Hyung

# Changes from -01 to -02:

- The new version focuses on the applicability of using SNMPv3 “as is” on 6LoWPANs.
- The goal is to describe how to utilize SNMPv3 without protocol modifications to take care of the constraints of 6LoWPAN nodes/links.

# Why SNMP

- Protocol Maturity
  - SNMP is the IETF's full standard management protocol
  - Significant experiences in implementation and operation
  - Many development libraries for almost all programming languages
  - Established network management tools exist e.g., HP OpenView, IBM Tivoli, Ganglia, Nagios, Cacti, etc
- Data Naming
  - SNMP provides a hierarchical namespace utilizing object identifiers (OIDs) for data naming purposes
- Data Retrieval
  - Supports read / write class operations and event notifications
- Security
  - SNMPv3 provides both message-level and transport-layer security

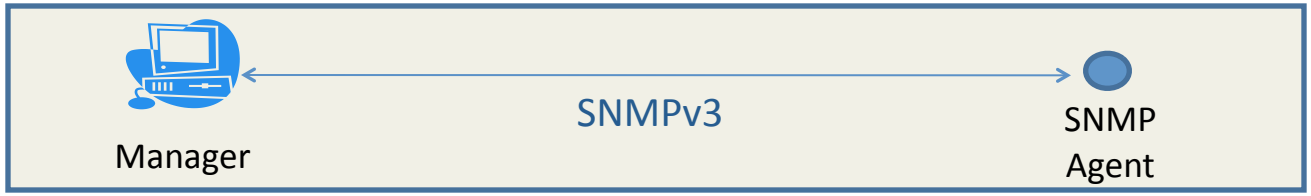
# Little-known SNMP Concepts: Contexts

- A context is a collection of management information accessible by an SNMP entity
- Think: One MIB tree out of several MIB trees accessible by an SNMP agent
- In order to identify an individual MIB object within the management domain, the SNMP entity's context is identified first (using the engine identifier and context name) followed by the object type and instance.

# Little-known SNMP Concepts: Proxies

- An SNMP proxy forwards SNMP messages to other SNMP engines.
- The forwarding is based on contexts and it is irrespective of the management objects being accessed.
- The SNMP proxy **cannot** be used for translation of SNMP requests into operations of a non-SNMP protocol.

# SNMP on 6LoWPANs




Lightweight End-to-End


Proxy Model


SNMP with Sub-Agent Protocols

# SNMP fits 6LoWPAN packets

- SNMP transports define the minimum message size implementations have to support
  - For SNMP over UDP, this size is 484 octets
- A minimum SNMPv3/USM/UDP noAuth/noPriv header is 67 bytes
- A minimum SNMPv3/TSM/DTLS/UDP auth/Priv header is 59 bytes
- A minimum SNMPv3/TSM/UDP NoAuth/NoPriv header is 46 bytes
- A minimum (historic) SNMPv1/UDP noAuth/noPriv header is 20 bytes

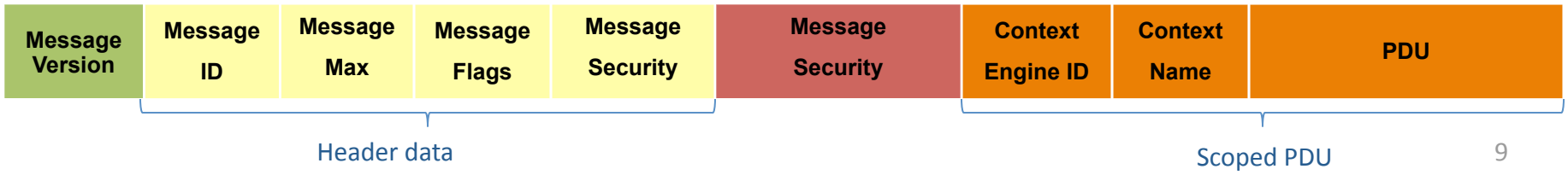
# SNMP Agent considerations

- Implementation of Access Control features
  - It is possible to support hardwired authorization tables, distinguishing only read and write access

- SNMPv3 Security
  - USM is a shared secret scheme which uses message-driven security; it is designed to be independent of other security infrastructures
  - TSM allows security to be provided by a secure transport protocol; enabling the use of TLS, **DTLS** and SSH

# Tradeoff of SNMP security

- Overhead of SNMP security
  - Tradeoff of message size and session establishment between message-driven security and transport-driven security
  - For USM, the security parameters are carried in each message, whereas they are associated with sessions in case of TSM
  - Minimum SNMPv3 packet overhead (without var-bind)
    - SNMPv3Message (USM) 67 octets (noAuthNoPriv)
    - SNMPv3Message (TSM) 59 octets (authPriv)
      - TSM has additional session establishment overhead



# Manager Implementation Considerations

- Data Retrieval
  - Polling
  - Pushing
  - Trap-directed polling
- Support for SNMP Proxies
  - In 6LoWPAN networks proxies may be used to
    - Change message encoding
    - Translate between SNMP versions
    - Work with a different security domain at the 6LoWPAN side of the network
    - Stateless compression of SNMP header

# Deployment Considerations

- Naming Issues
- Usage of SNMP Protocol Operations
- Timeouts and Retransmissions
- Suitable Polling Intervals
- Caching Issues

# Applicable Standardized MIBs

- Entity Sensor MIB [RFC3433] defines objects for information that is associated with physical sensors
  - e.g. the current value of the sensor, operational status, and the data units and precision associated with the sensor
  - It can be reused for 6LoWPANs (and may also be applicable to SE2.0)

# SNMP with DTLS

- DTLS Handshake
  - With ECC cipher suites e.g. ECMQV_ECQV certificates [I-D.draft-campagna-tls-ecmqv-ecqv-00]
- Message overhead after the key exchange
  - Min SNMPv3 TSM overhead: 46 bytes
  - DTLS transport layer overhead: 13 bytes
  - To retrieve sysUpTime (1.3.6.1.2.1.1.3) using SNMPv3/TSM over DTLS over UDP, the message size is roughly 73 bytes

# Conclusion

- The draft covers the applicability of SNMPv3 for 6LoWPANs.
- SNMPv3 would work on 6LoWPAN without any modification to the protocol.
- Stateless compression analogous to 6LoWPAN HC may further reduce the header size.

# References


RFC 3411: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

RFC 3412: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

RFC 3413: Simple Network Management Protocol (SNMP) Applications

RFC 3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

RFC 3415: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

RFC 3416: Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

RFC 3417: Transport Mappings for the Simple Network Management Protocol (SNMP)

RFC 5591: Transport Security Model for the Simple Network Management Protocol (SNMP)

ID-SNMP-DTLS: Transport Layer Security Transport Model for SNMP <draft-ietf-isms-dtls-tm-01.txt>

ID-SNMP-OPTS: SNMP Optimizations for 6LoWPAN <draft-hamid-6lowpan-snmp-optimizations-02.txt>

# Appendix: SNMP Concepts- Subagents

- An SNMP subagent provides information to an SNMP agent using a subagent protocol that can use different message formats
- The subagent registers which objects it likes to be responsible for while the SNMP master agent takes care to forward retrieval requests to the subagents as needed to process SNMP queries
- Subagents are used in modular routers to export data from pluggable line cards or daemons to the SNMP agent running on the main processor

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |

# draft-ietf-6lowpan-nd-07

Authors:
Zach Shelby (ed.)
Jonathan Hui
Pascal Thubert
Samita Chakrabarti
Erik Nordmark
Carsten Bormann

# Outline

- What is 6LoWPAN-ND (in 1 slide)
- Current status
- Changes since IETF-75 (-05 to -07)
- See the end of this slide-set for reference slides

# 6LoWPAN Neighbor Discovery

- Optimizes ND with a new mechanism for LoWPANs
  - Enables sufficient LoWPAN operation on its own
    - Other ND mechanism (e.g. RFC4861 may also be used)
  - Optimizes the host-router interface
  - Node Registration mechanism
    - Provides DAD, AR and NUD using that mechanism
- Multihop router and context information dissemination
- Compatible with link-layer mesh and IP routing
- Support for simple, extended and ad-hoc LoWPANs
- Fault tolerance and duplicate identifier detection

# Current status

- Draft was accepted as a WG doc in IETF-73
  - Combination of 5 drafts
- 3 new revisions since IETF-75
- Message in IETF-75 was “Get it done”
- Current status:
  - Draft is technically stable
    - Only minor technical changes since -05
  - Enabled co-existence with other ND mechanisms in -07
  - Major editorial improvements in -07

# Changes from -04 to -05

- Meaning of the RA's M-bit changed to original [RFC4861] meaning (#46).
- Terms "local" and "non-local" included.
- Next-hop determination text simplified (#49).
- Neighbor cache and destination cache removed.
- IID to link-layer address requirement relaxed.
- NR/NC changes to enable local refresh with routers (#48).
- Modified 6LoWPAN Information Option (#47).
- Added a Protocol Constants section (#24)
- Added the NR processing table (#51)
- Considered the use of SeND on backbone NS/NA messages (#50)

# Changes from -05 to -06

- Fixed the Prf codes (#52).
- Corrected the OIIO TID field to 8-bits.  Changed the Nonce/OII order in both the OIIO and the NR/NC. (#53)
- Corrected an error in Table 1 (#54).
- Fixed asymmetric and a misplaced transient in the 6LoWPAN terminology section.
- Added Updates RFC4944 to the header

# Changes from -06 to -07

- Updated addressing and address resolution (#60).
- Changed the Address Option to 6LoWPAN Address Option, fixed S values (#61).
- Added support for classic RFC4861 RA Prefix Information messages to be processed (#62).
- Added a section on using 6LoWPAN-ND under a hard-wired RFC4861 stack (#63).
- Updated the NR/NC message with a new Router flag, combined the Code and Status fields into one byte, and added the capability to carry 6IOs (#64).
- Made co-existence with other ND mechanisms clear (#59).
- Added a new Protocol Specification section with all mechanisms specified there (#59).
- Removed dependencies and conflicts with RFC4861 wherever possible (#59).

# Recent issues

- How to use 6LoWPAN-ND with a hard-wired RFC4861 IPv6 stack (e.g. a Linux ER)
  - Covered in -07, see Section 10
- Co-existence with RFC4861
  - -07 allows RFC4861 to be used in addition
  - Many places preventing this were fixed in -07!
- Are we re-defining RFC4861?
  - No! -07 is a new ND mechanism, optimized for LoWPANs.
- Samita asked if we should split this into two documents (basic, extended)?

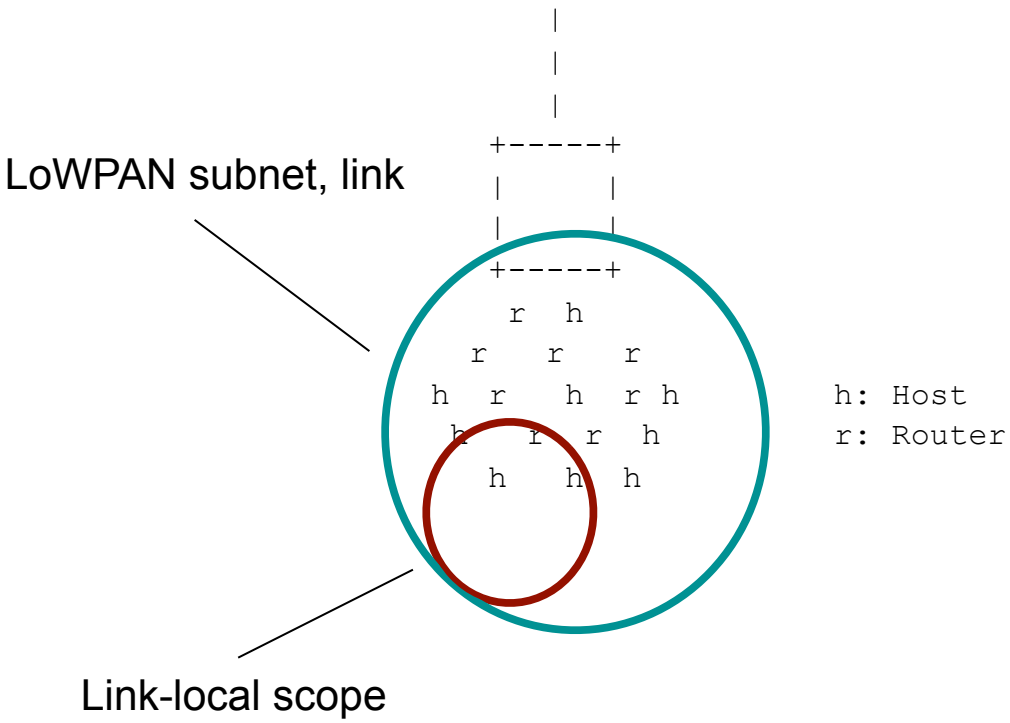
# Next steps

- Working with 6man
- -07 addresses most comments from the list
- Now to weed out final bugs and nits
- -08 expected within 3 weeks of the IETF

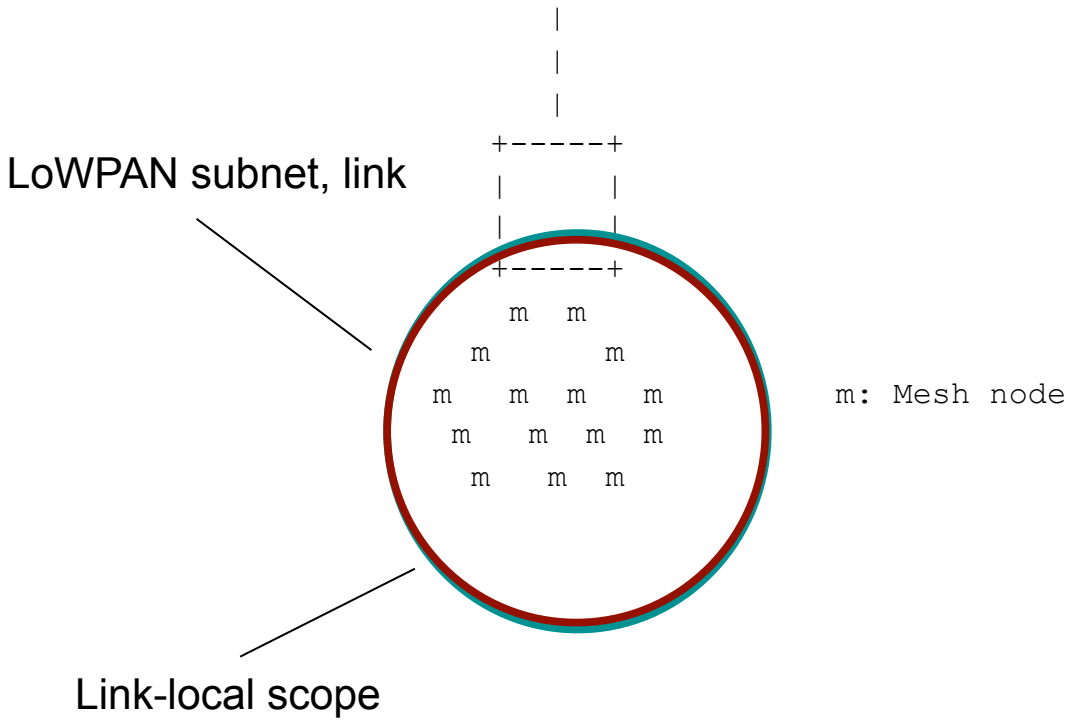
# Reference slides

draft-ietf-6lowpan-nd-07

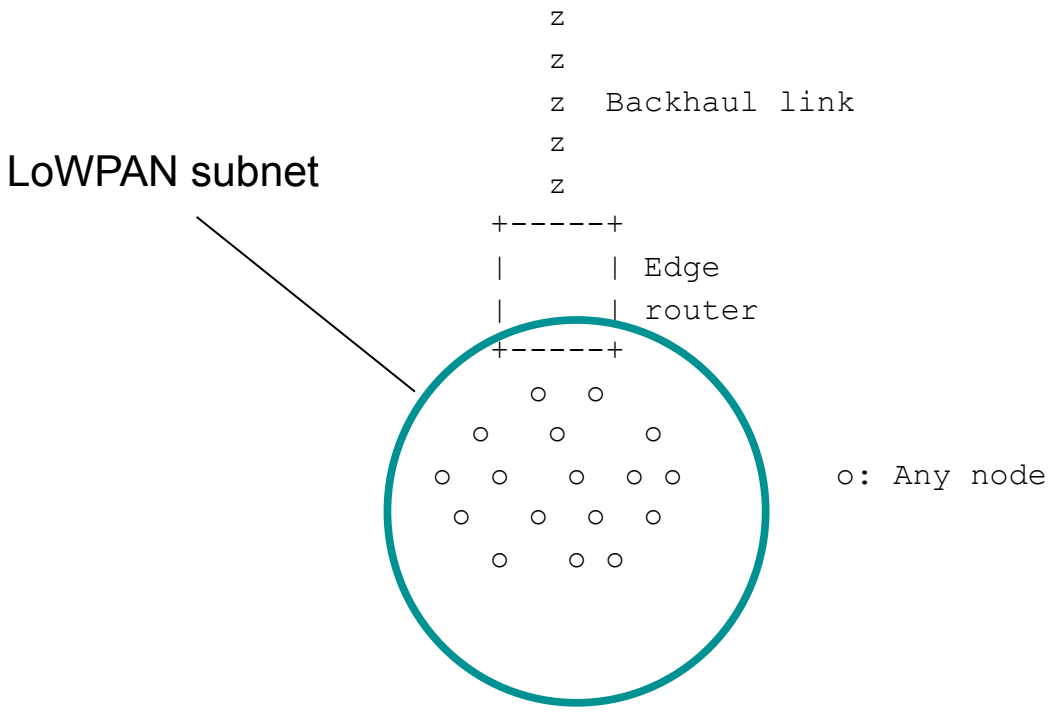
# Architecture - Route Over



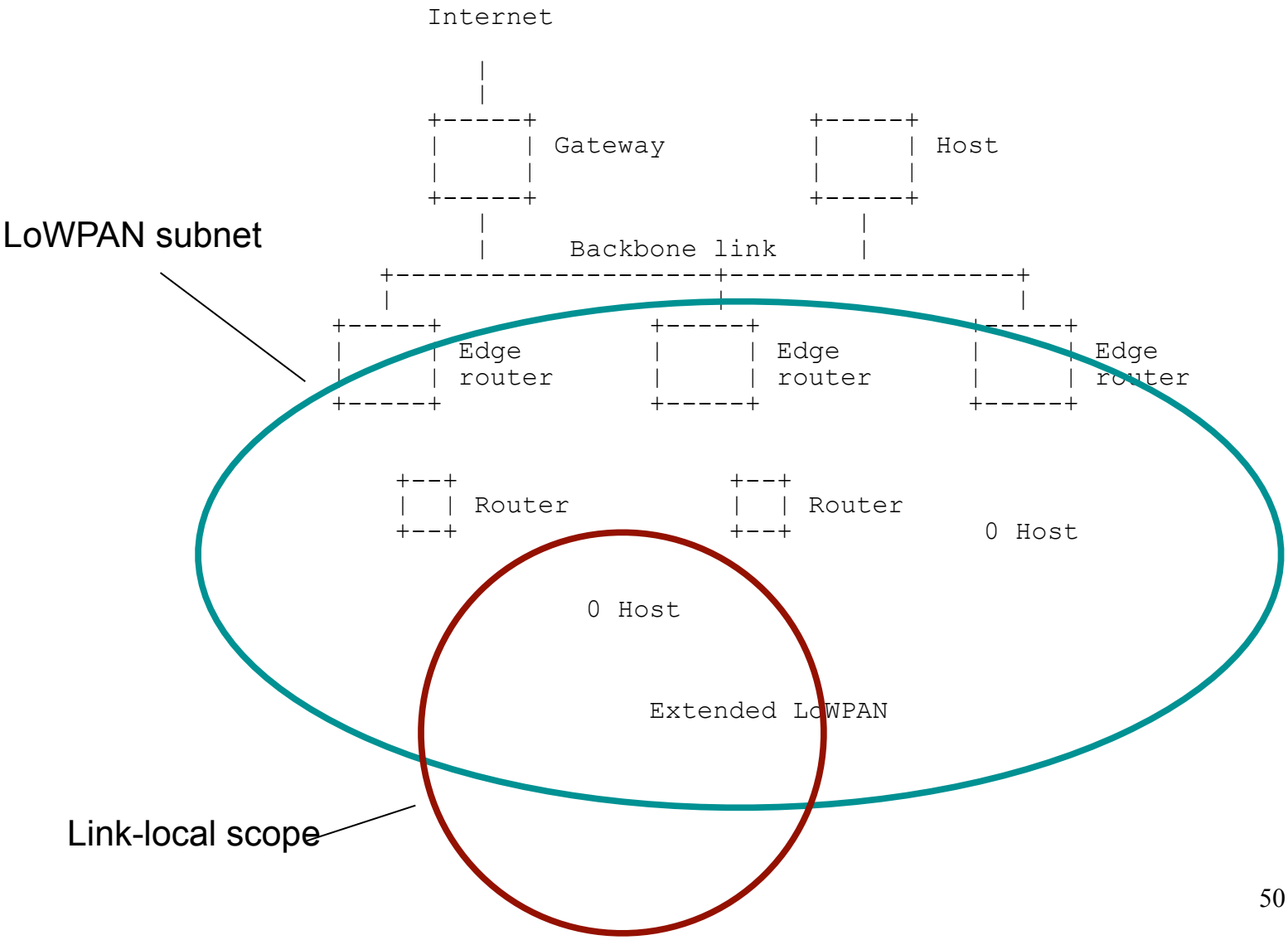
# Architecture – Mesh Under



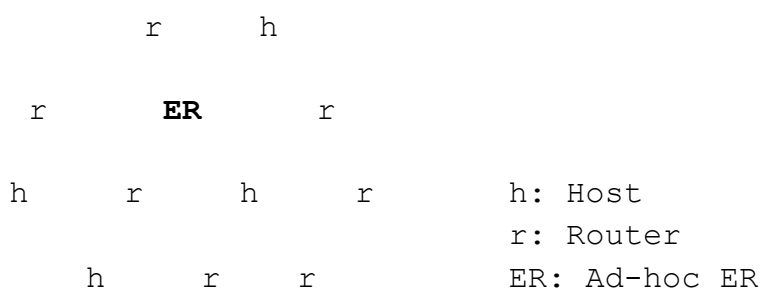
# Architecture – Single LoWPAN



# Architecture – Extended LoWPAN

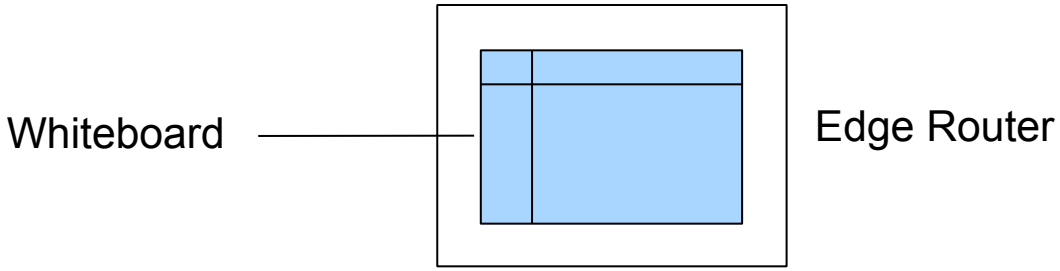


# Ad-hoc LoWPANs



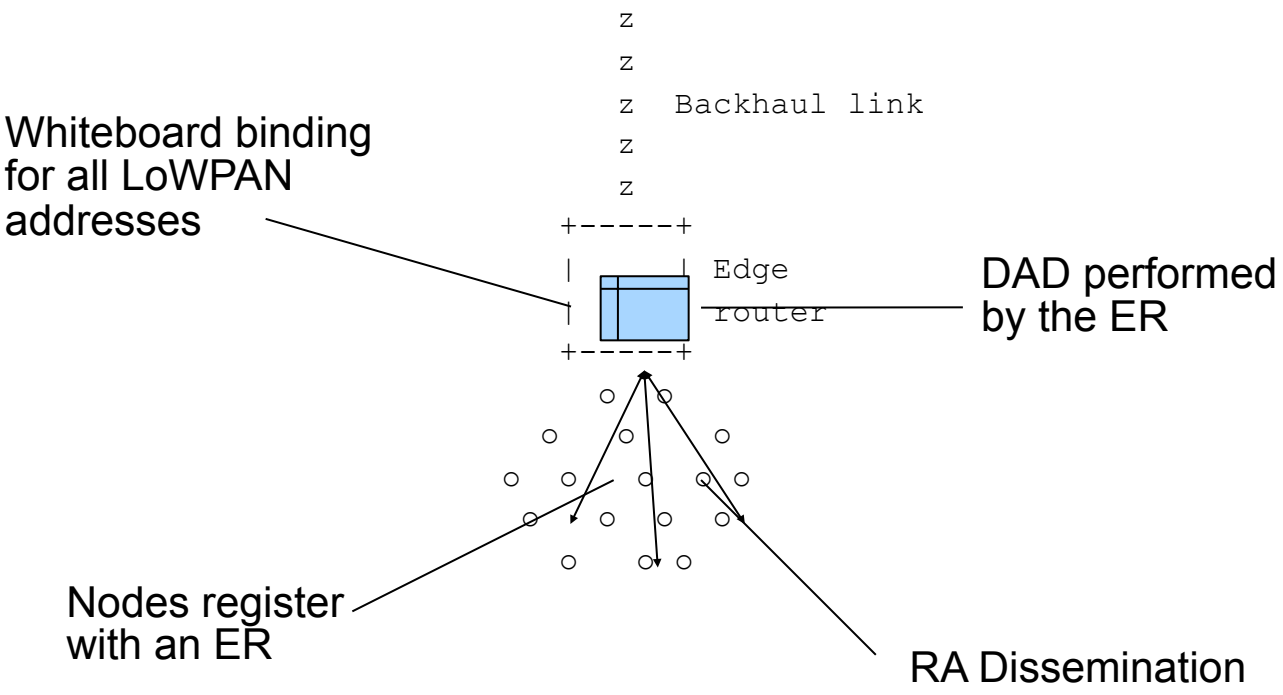

- Ad-hoc use of ND for 6lowpan defined
  - Almost identical to simple LoWPAN operation
  - 100% transparent to LoWPAN nodes
  - ER generates ULA [RFC4193] and disseminates it
  - Whiteboard state can be optimized

# Whiteboard model

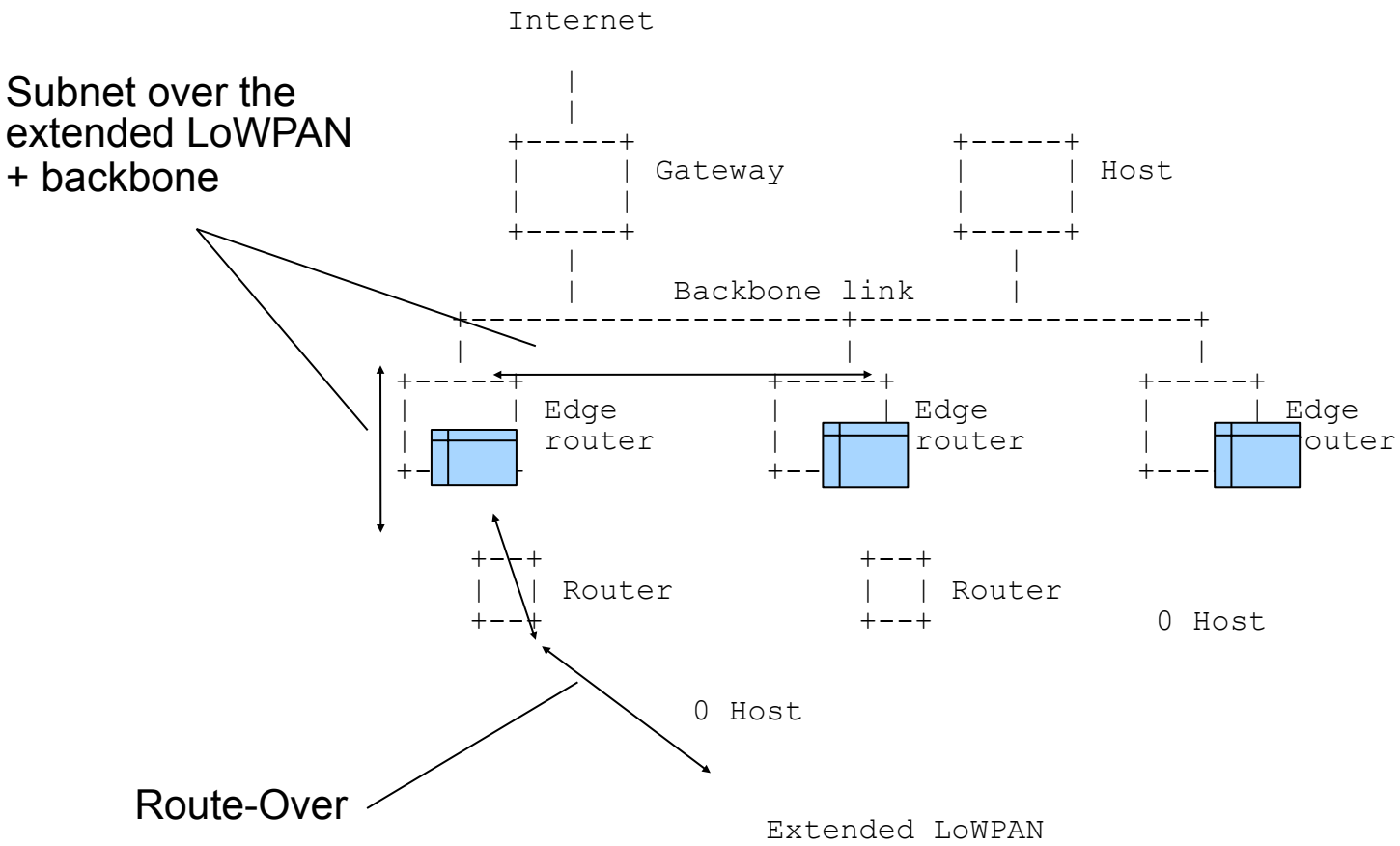



- A whiteboard binding entry has the following fields:
  - `Owner Interface Identifier`
  - `IPv6 Address`
  - `TID, Nonce, Lifetime`
- Bindings are soft
  - Must be refreshed
  - Can be moved between ERs

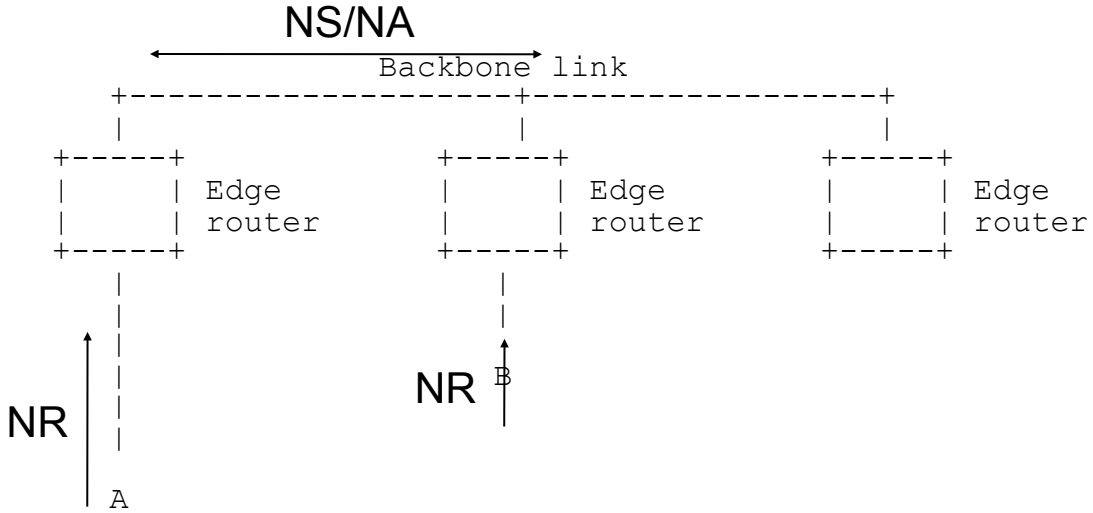
# Basic features



# Optional features



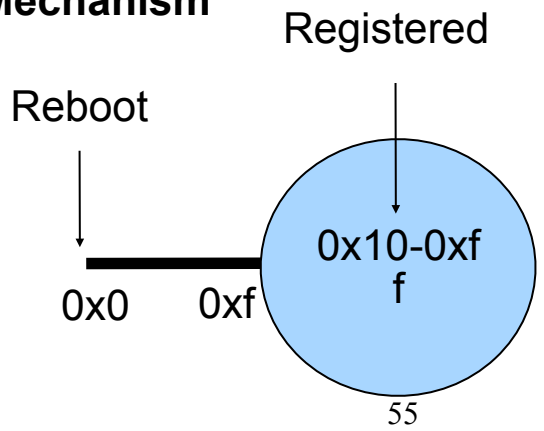
# Duplicate identifier detection




**NR message contents:**

- Owner Interface Identifier (64-bit)
- Nonce (32-bit)
- Transaction ID (8-bit)
- Addresses to register

**TID Lollypop Mechanism**

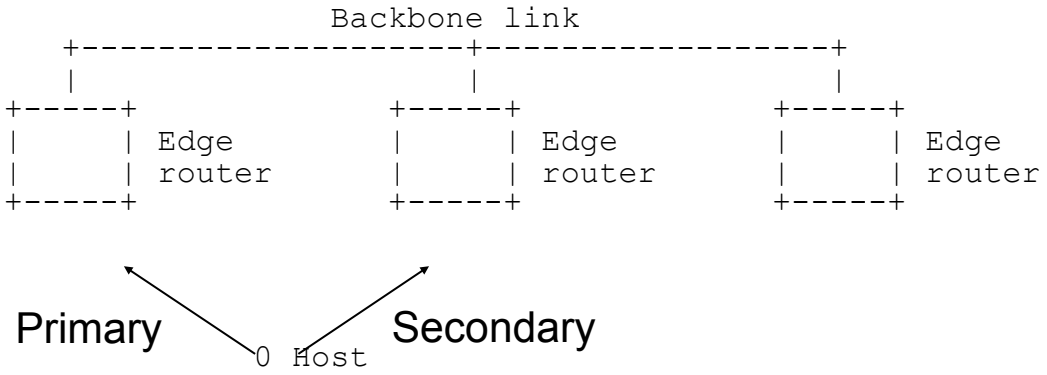


# NR message processing

| Type | OII | Nonce | TID | Address | Action |
|---|---|---|---|---|---|
| Initial Registration | Unique | * | * | Unique | Accept |
| New Address or Movement | Duplicate | Same | > | * | Accept |
| Duplicate message | Duplicate | Same | <= | * | Ignore |
| Duplicate message | Duplicate | Same | <= | * | Ignore |
| Node Reboot | Duplicate | Different | < 0x10 | * | Accept |
| OII Collision | Duplicate | Different | > 0xf | * | Reject |

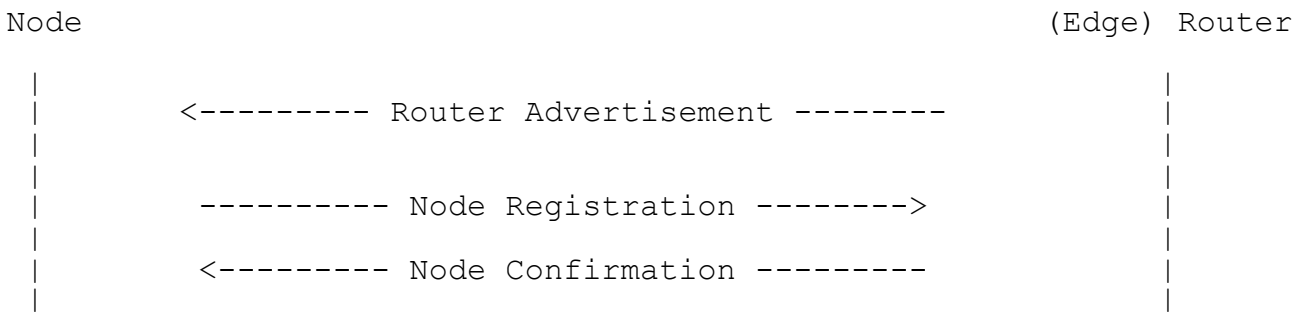
* = Wildcard

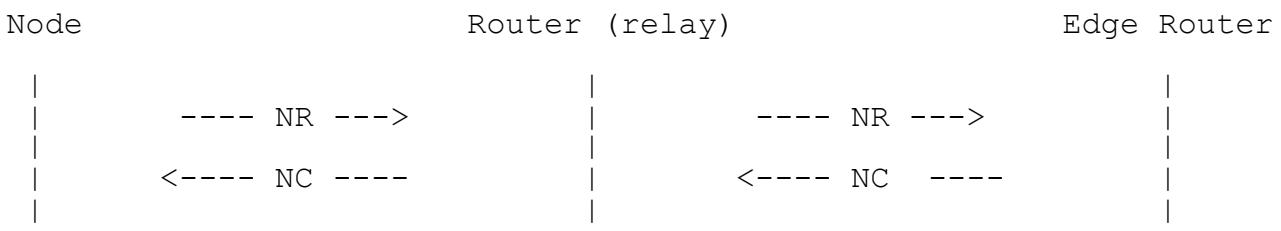
# Fault tolerance




- Edge Router recovery
- Use of secondary registrations for fault tolerance
  - Prepare network state for movement to new primary
  - Automatic primary->secondary backup operation
  - Bicasting possible

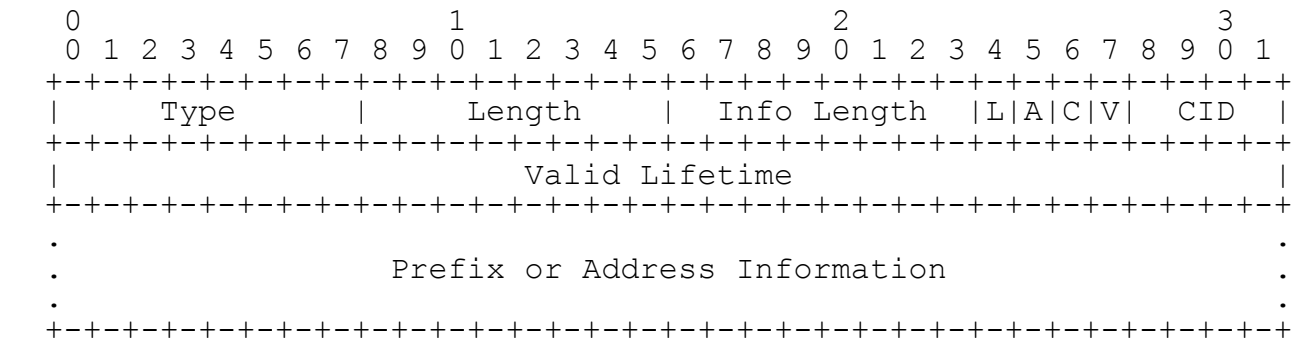
# Message exchanges



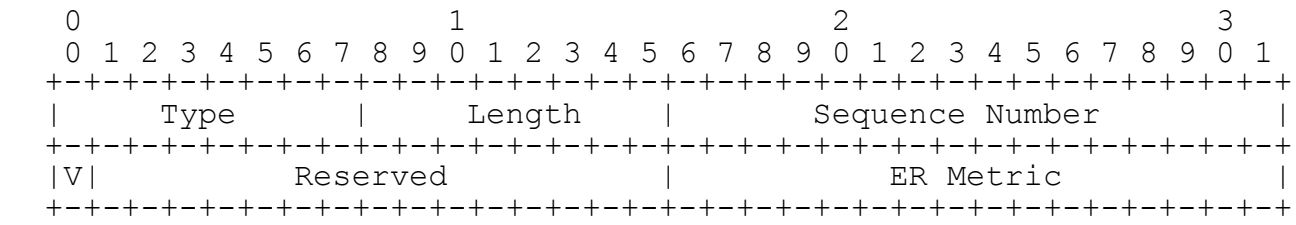
# RA options

**6LoWPAN Information Option**

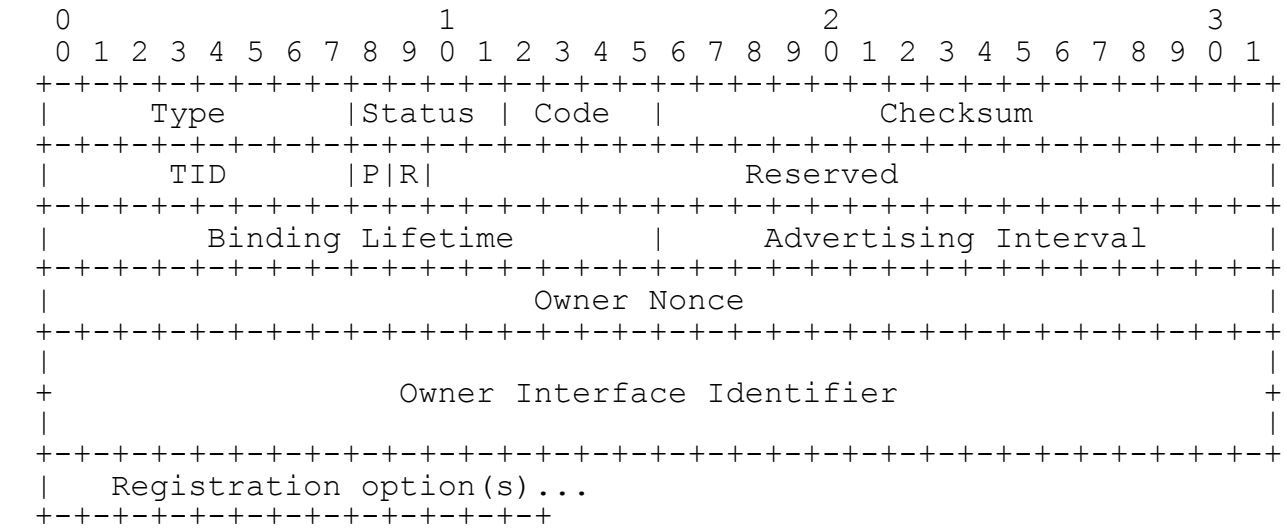



**CID** – Context Identifier for use in 6LoWPAN HC compression.

**6LoWPAN Summary Option**



# NR/NC message



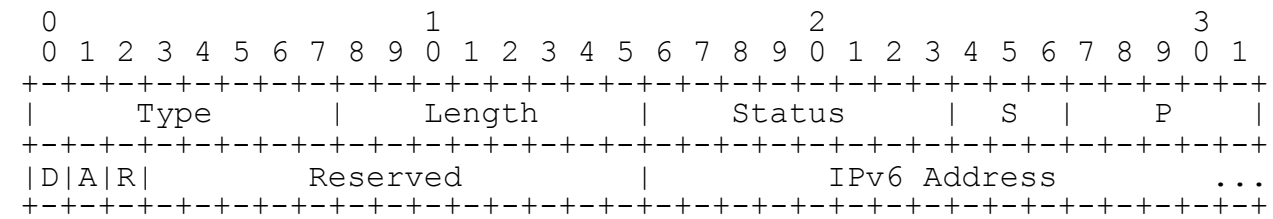

**TID** – Transaction ID for matching confirmations.

**P** – Primary flag for using an ER as primary. For use with secondary registrations.

**R** – Indicates if the registering node is a host or router.

# NR/NC options

**Address Option**




**P/S** – Prefix and suffix compression fields.

**D** – Allow duplicates flag.

**A** – Address request flag.

**R** – Remove address flag.

**Source link-layer address option [RFC4861, RFC4944]**

**Target link-layer address option [RFC4861, RFC4944]**

# 76th IETF: 6lowpan WG Agenda

| | | |
|---|---|---|
| 13:00 | Introduction | Chairs (5) |
| 13:05 | 4 – Routing Requirements | Chairs (5) |
| 13:10 | 5 – Use cases | Chairs (5) |
| 13:15 | 2 – HC | Chairs/JH (5) |
| 13:20 | 6 – Security | Chairs/KK (5) |
| 13:25 | 0 – MIB | KK (5) |
| 13:30 | 0 – SNMP Opt | HM (15) |
| 13:45 | 1 – ND | ZS (35) |
| 14:20 | 6LowApp Pointer, New Work? | Chairs (5) |