Node ID Internetworking Architecture

Bengt Ahlgren (SICS), Jari Arkko (Ericsson),
Lars Eggert (NEC) and Jarno Rajahalme (Nokia)

9th IEEE Global Internet Symposium
Barcelona, Catalunya, Spain, April 28-29, 2006

Background

- IPv4 once "solved" the internetworking problem
  - long ago and in an Internet far, far away
- but the problem has gradually become "unsolved"
  - NATs, firewalls and other middleboxes
  - IPv4 address space shortage
  - harmful traffic, need for controlled transparency
  - increasing mobility, both hosts & networks

So What About IPv6?

- IPv6 is not an alternative
  - many of the same shortcomings
  - we haven’t managed to migrate to it
  - huge investment in IPv4 infrastructure
  - middleboxes are here to stay:
    people <u>want</u> them
- time for a new “network of networks”

Architectural Goals

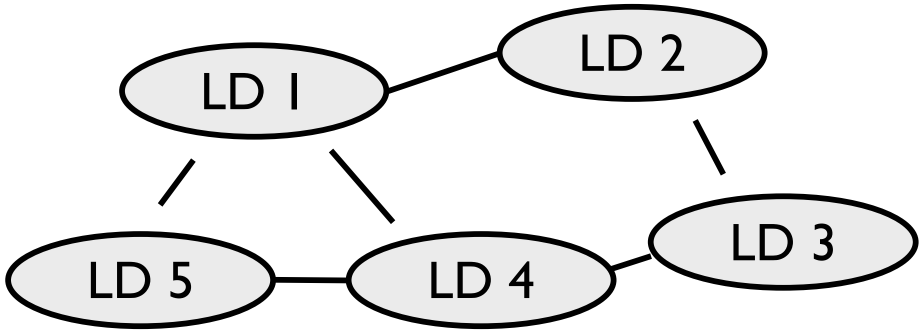
- must integrate heterogeneous domains
- require minimal set of common pieces, e.g., avoid new global address spaces
- need strong migration incentives (cf. IPv6)
  - built-in mobility
  - always-on security, DoS protection, privacy
  - immediate benefit from partial deployment

Fundamental Features

1. separation of node identity and node location(s)
    - addresses are only used as locators
    - a node's locators can change over time
    - a node's locator <u>types</u> can change over time
2. cryptographic node identities
    - public key represents node identity (NID)
    - NID hash used as forwarding token
3. communication establishment through explicit rendezvous points

Assumptions

- world consists of independent <u>locator domains</u>
- LDs are self-contained with coherent internal addressing and routing between their nodes



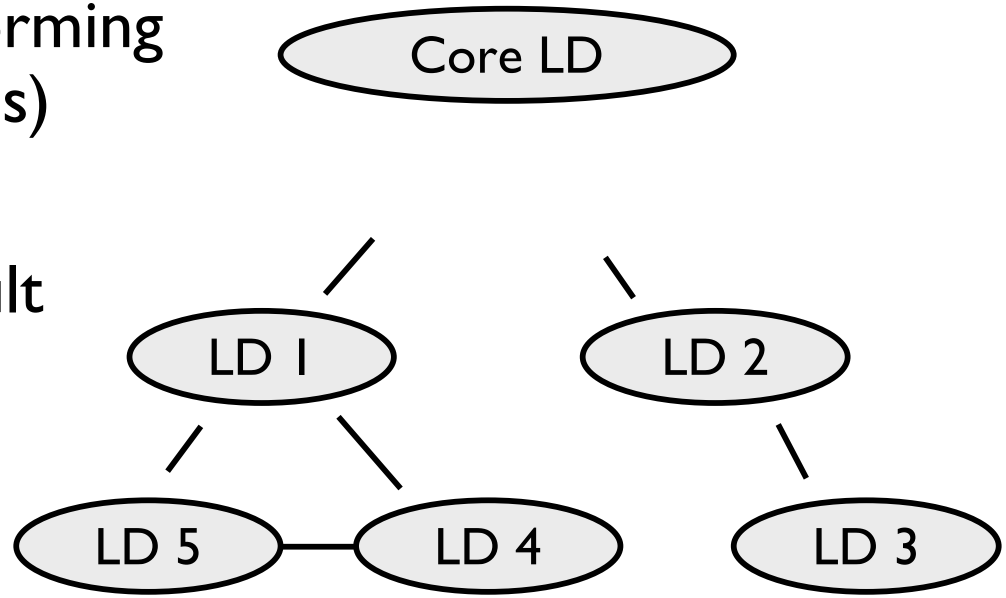
- connectivity between LDs is dynamic
- connectivity that ties nodes into LDs is dynamic
- result: very, very, very hard routing problem
  - BGP-like routing infeasible due to scale, dynamics and structure

Observation

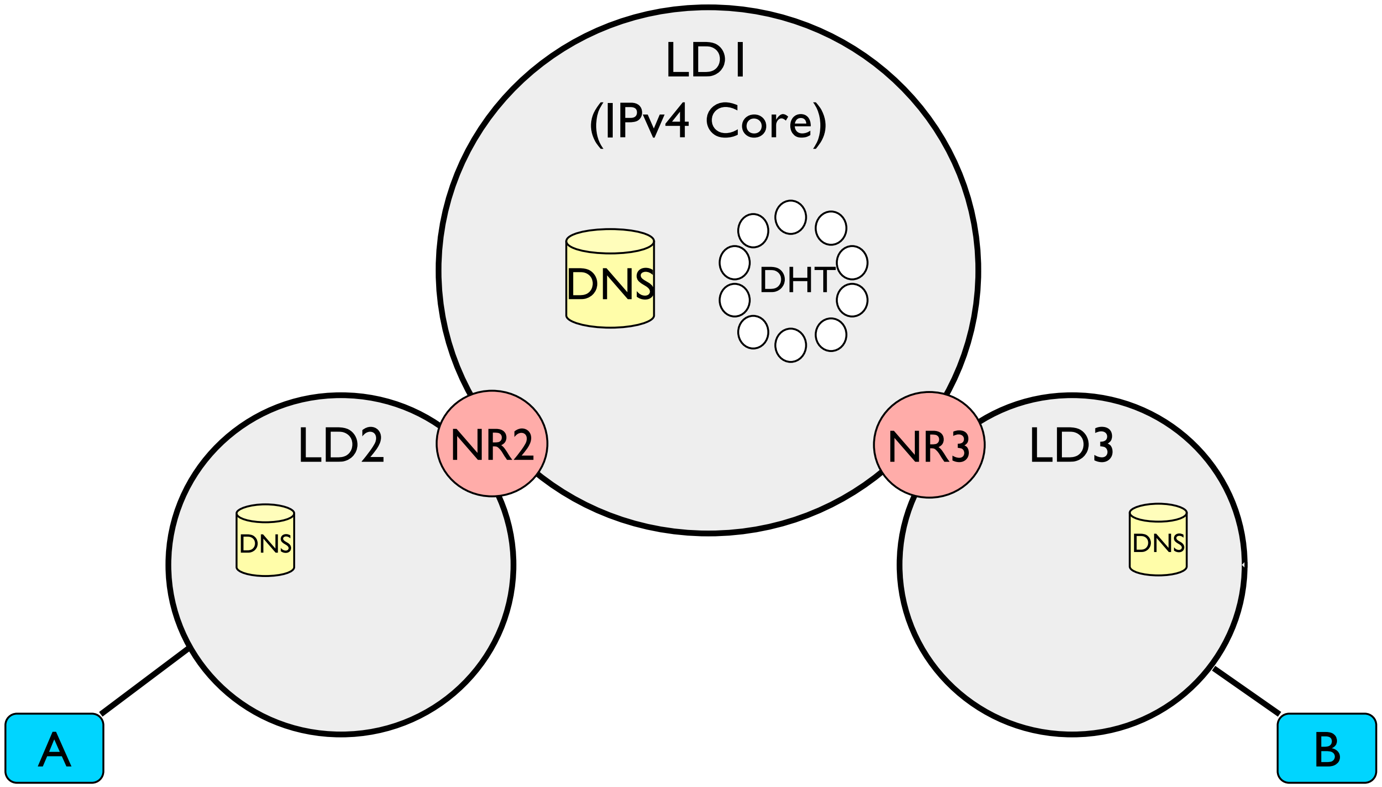
- dynamic events happen most frequently towards the edge of the topology
  - host and stub network mobility and multihoming
  - core networks (LDs) are tightly controlled and mostly statically interconnected
- NID architecture hinges on this observation!

Consequences

- we assume a small number of "core" backbone LDs
- other LDs dynamically attach to the cores
- and to each other, forming tree-like stubs (DAGs)
- routing in those "stub trees" by default is towards the core
- otherwise little constraints

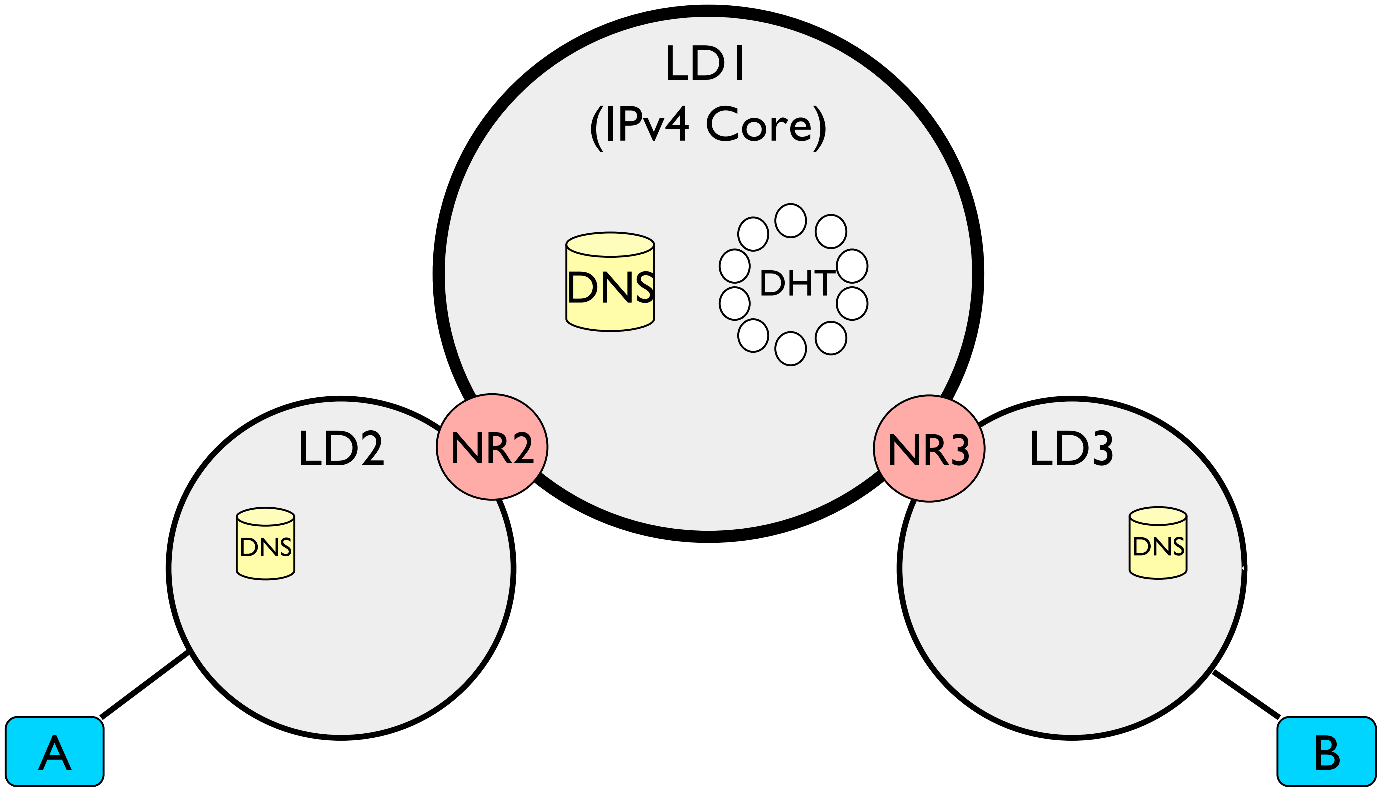


Example



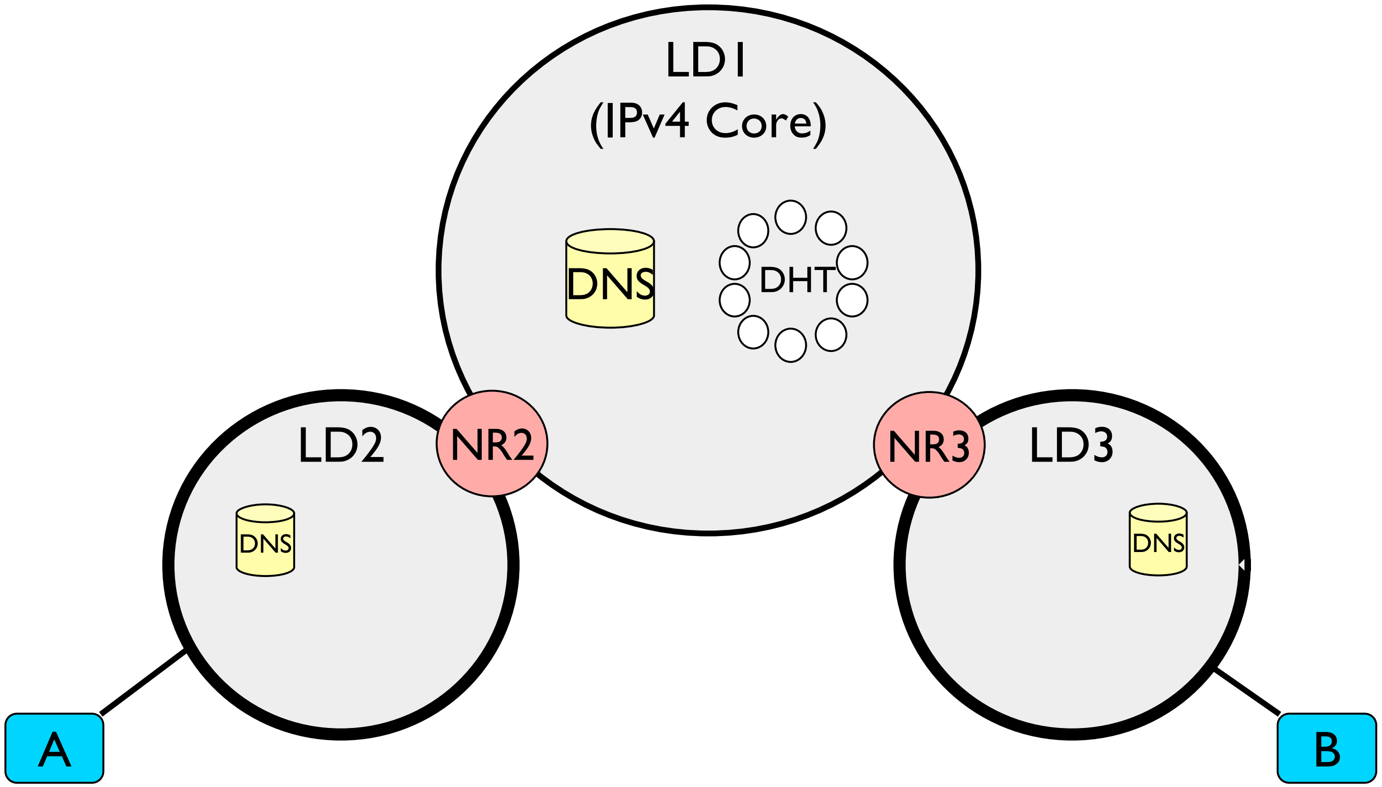
Example

We assume a core network (or a few core networks).
For instance, the IPv4 and IPv6 core networks.



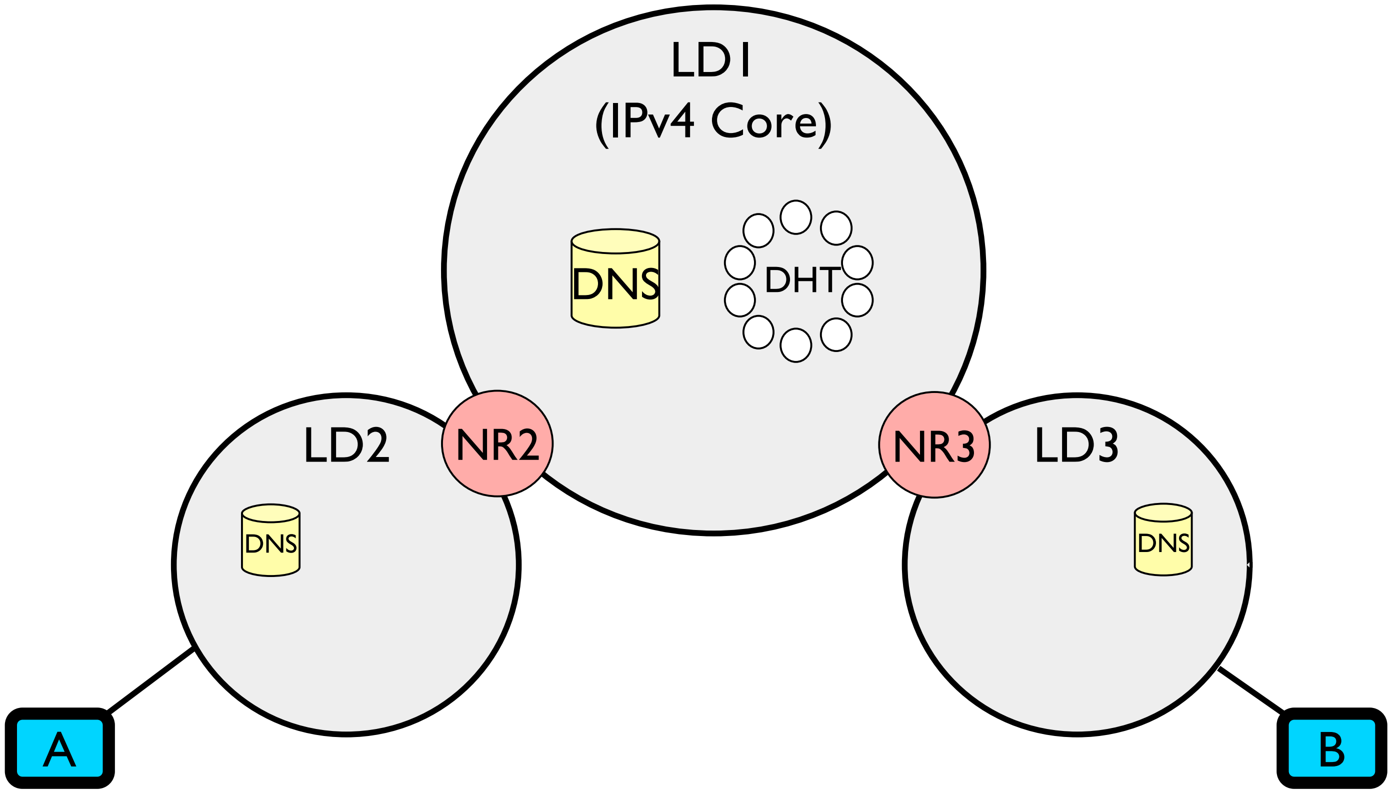
Example

Different locator domains, e.g., LD2 and LD3, use their own addressing and internal routing schemes.



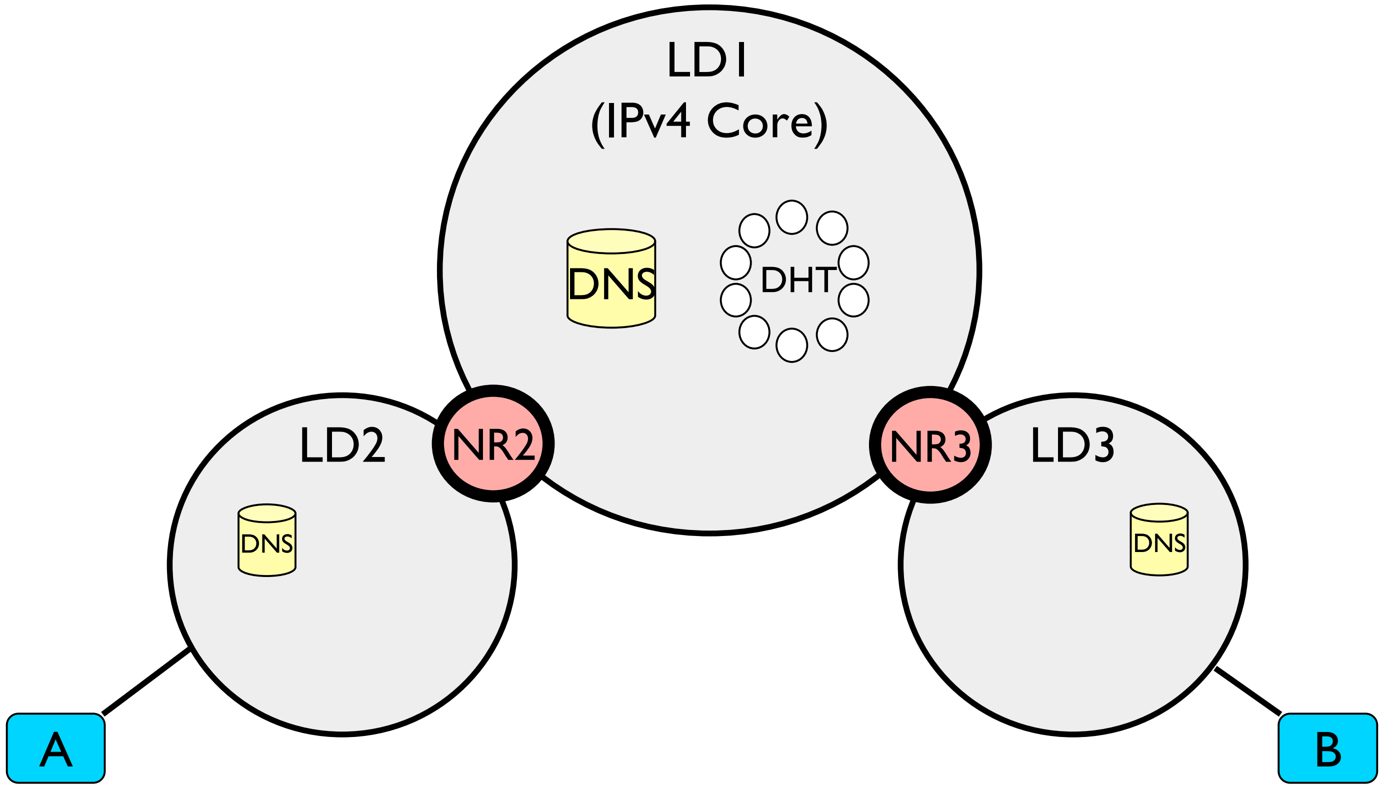
Example

Nodes have Node Identities (NIDs), which consist of the public key of the node. These keys can be self-generated.



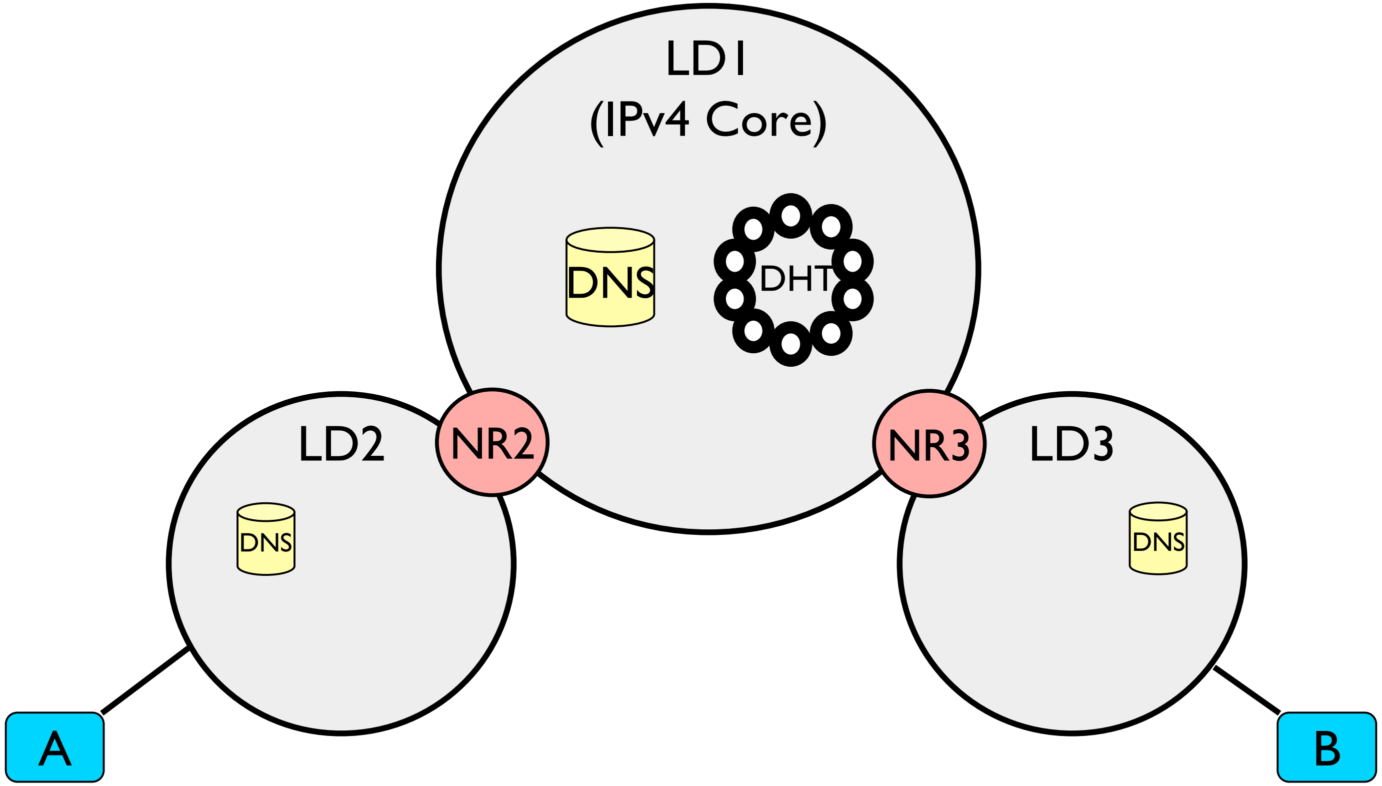
Example

Domains are connected via NID Routers (NRs). These perform routing based on the destination NID, as well as locator mapping.



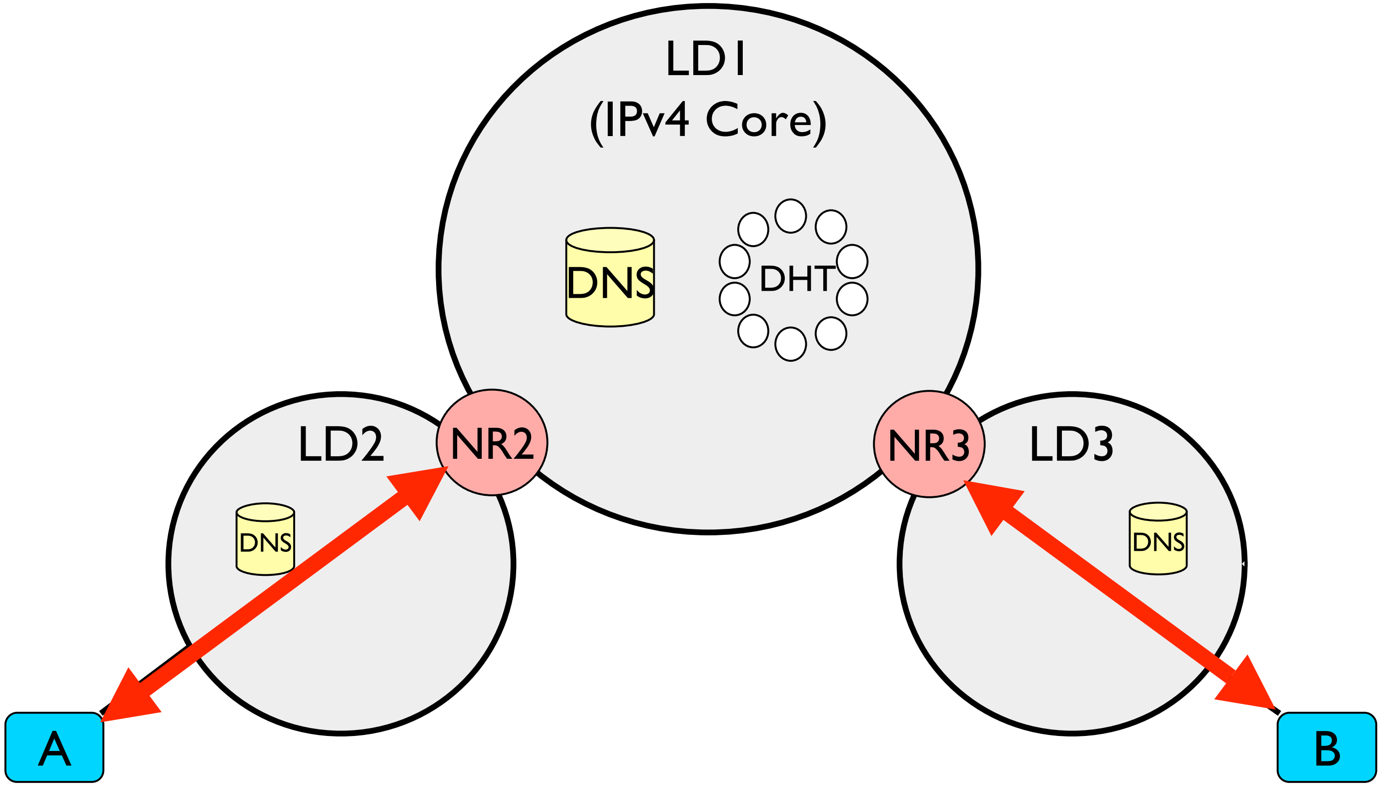
Example

Core LDs maintain a database that contains the locators for each NID router connected to them. (It does not hold per-node state.)



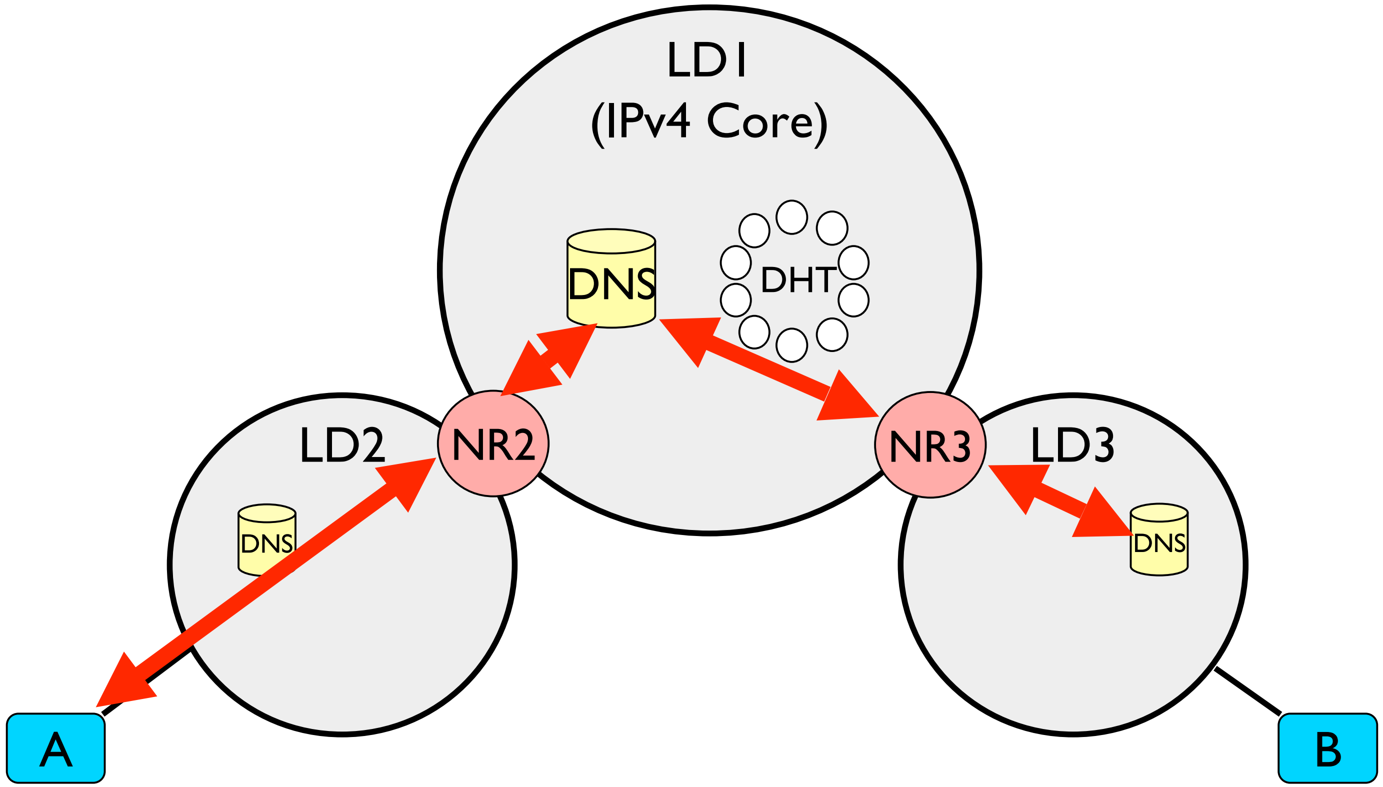
Example

Nodes A and B arrive in their LDs, register their NIDs and locators with the LD's NID routers – NR2 and NR3 in this case.



Example

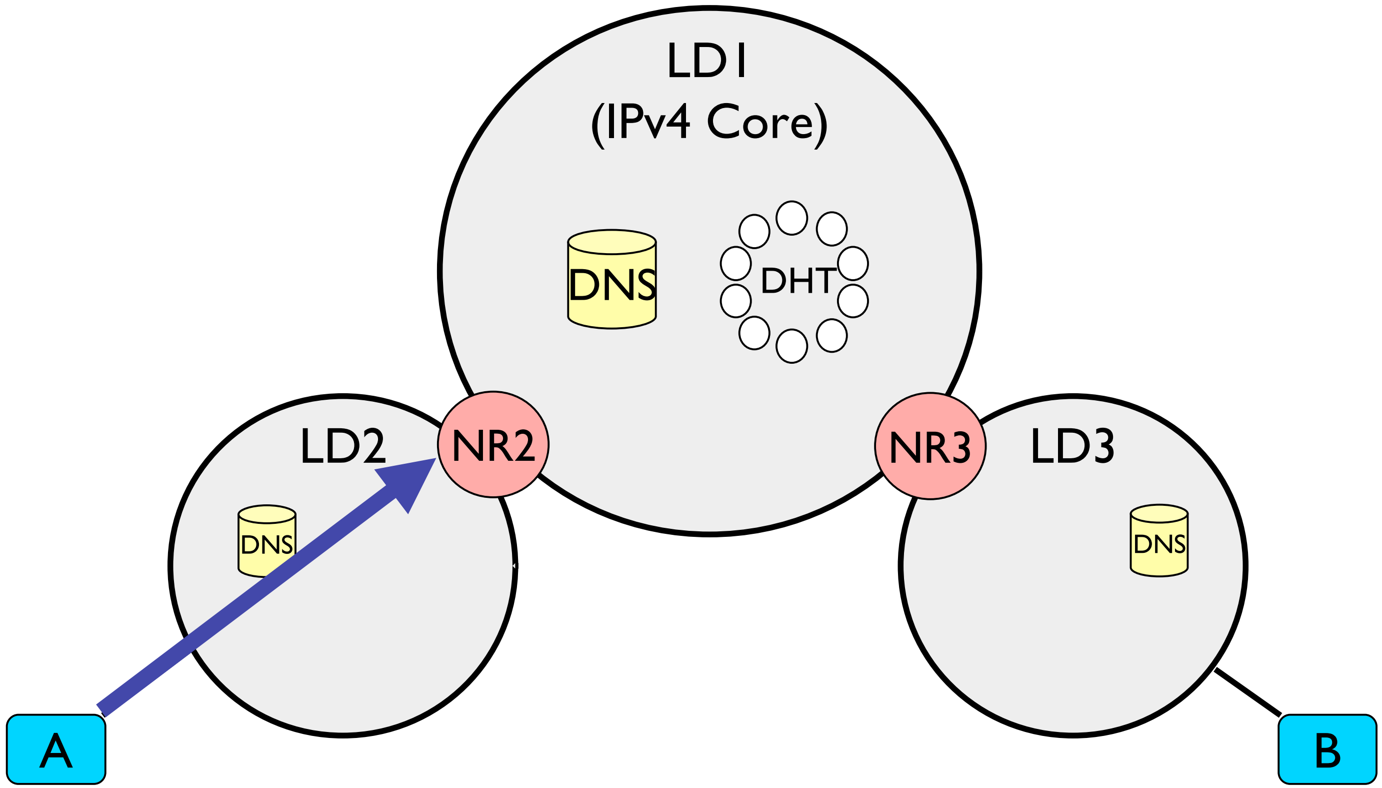
When A contacts B, it resolves B's DNS name. The result contains the NIDs of B (NID_B) and the NID of B's rendezvous point (NID_{NR3}).



Example

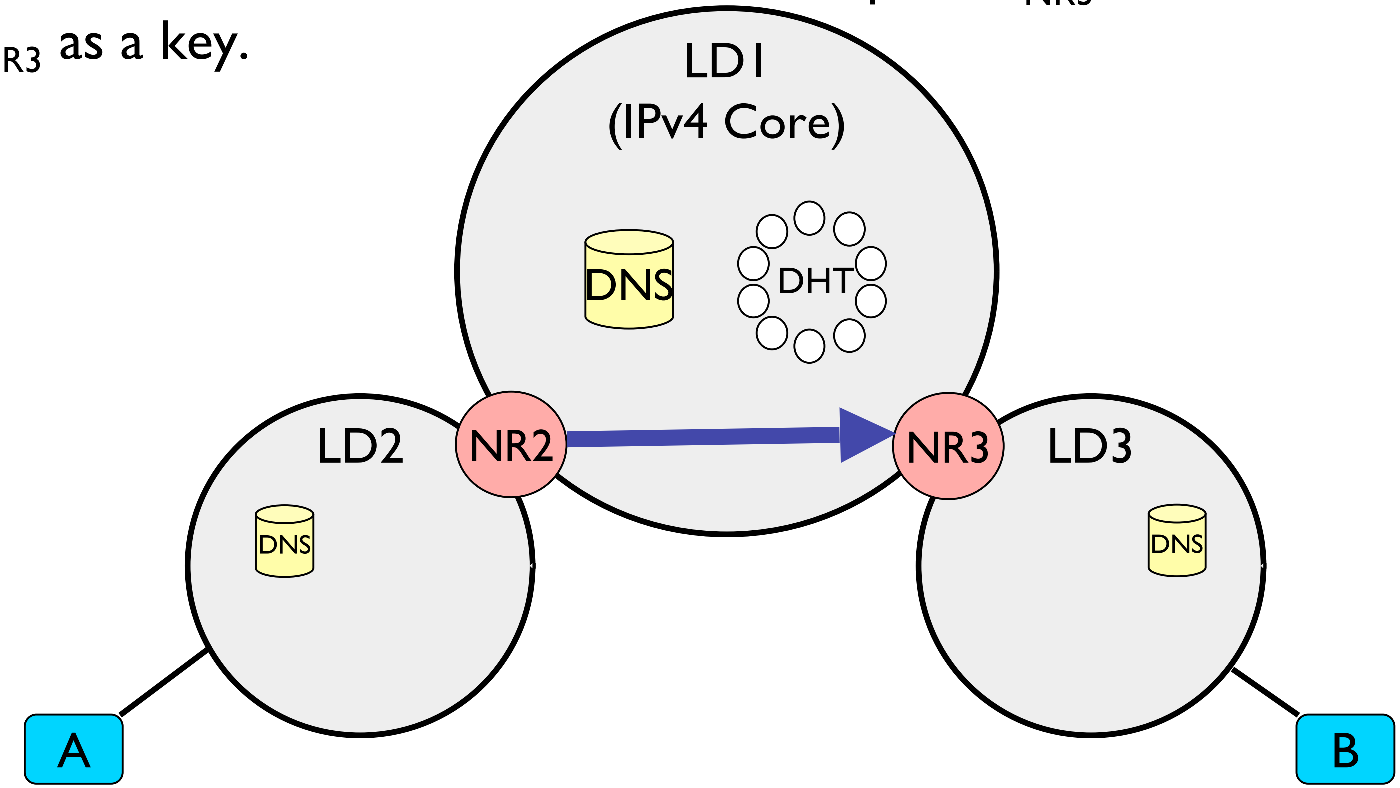
Now A can send its first packet to B:

LD Header	Node ID Header	Payload
Destination = NR2	Destination NID = B Destination NR = NR3	...



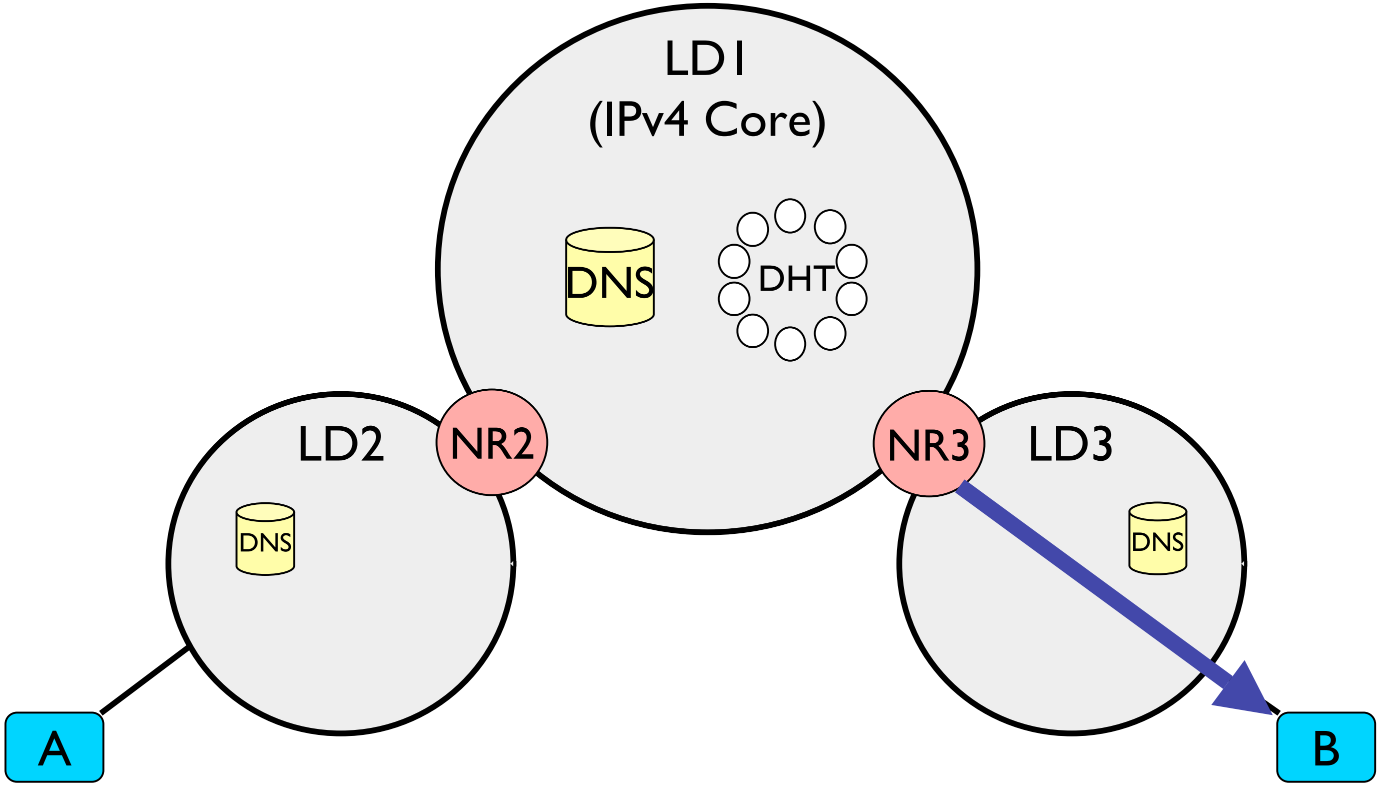
Example

If NR2 knows NID_B locally, it forwards it locally in LD2. Otherwise it forwards it along the default route up. However, since NR2 is at the core, it doesn't have a default route. So it looks up LOC_{NR3} from the DHT using NID_{NR3} as a key.



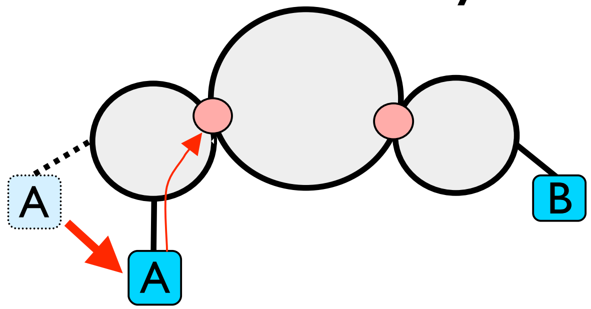
Example

NR3 knows NID_B locally, so it forwards the packet to the B's address in LD3.

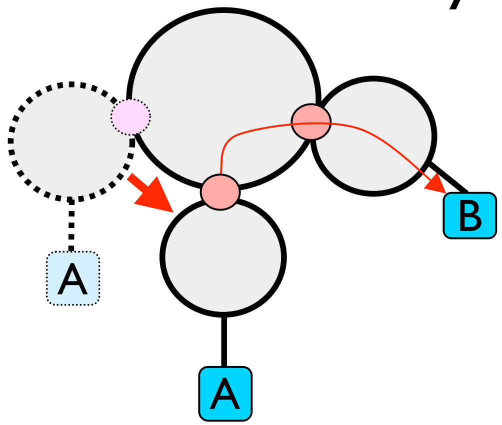


Mobility & Multihoming

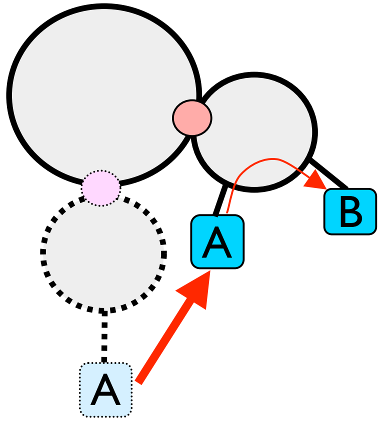
local mobility



network mobility



end-to-end mobility



Reality Check

- incremental deployment? - yep
  - attach NID routers to current core
- minimal required common pieces? - yep
  - node ID space
- inherent security? - yep
  - crypto NIDs, node location hidden
- mobility & multihoming? - yep
  - through NID/locator bindings

We Are Far From Done

- internetworking architecture based on node IDs
  - bridges heterogeneous locator domains
  - provides native mobility and compulsory security
- some current work items
  - details of “stub tree” DAG routing
  - remove reliance on DNS
  - stub operation when disconnected from core
  - prototyping in the “Ambient Networks” project